Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Escuela Académico Profesional de Ingeniería de Sistemas

Implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la invocación por protocolos. Caso de estudio: Municipalidad de Miraflores

TESIS

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Gino Brehan AGUILAR ALCARRÁZ

ASESOR

Percy Edwin DE LA CRUZ VÉLEZ DE VILLA

Lima, Perú

2016

Referencia bibliográfica

Aguilar, G. (2016). *Implementación de un modelo simplificado de firma digital basado en la tecnología PKI y la invocación por protocolos*. *Caso de estudio: Municipalidad de Miraflores*. [Tesis de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Académico Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

FICHA CATALOGRÁFICA

AGUILAR ALCARRÁZ, Gino Brehan

IMPLEMENTACIÓN DE UN MODELO SIMPLIFICADO DE FIRMA DIGITAL BASADO EN LA TECNOLOGÍA PKI Y LA INVOCACIÓN POR PROTOCOLOS. CASO DE ESTUDIO: MUNICIPALIDAD DE MIRAFLORES
Programa/Línea de investigación C.0.3.25 (Tecnología de información y aplicaciones de sistemas).
Lima, Perú 2014.

Tesis, Facultad de Ingeniería de Sistemas e Informática, Pregrado, Universidad Nacional Mayor de San Marcos.

DEDICATORIA:

Dedico este trabajo a mis padres, que me apoyaron siempre en mi formación, a mi hermano y a todos los que me brindaron su apoyo desinteresado.

AGRADECIMIENTOS

En primer lugar, a Dios.

A mis señores padres, Elizabeth y Raúl, de quienes recibí consejos y apoyo constantes desde mis primeros pasos hasta el día de hoy, y por siempre.

A mi hermano Joseph, quien no deja de sorprenderme con su habilidad y grado de análisis.

Al profesor, asesor y amigo, Percy Edwin De la Cruz Vélez de Villa, por su paciencia, orientación y apoyo incondicional en la elaboración del presente trabajo.

A los profesores de pregrado que me acompañaron a lo largo de la carrera, por sus conocimientos y lecciones impartidas.

A mis compañeros del trabajo, quienes día a día confían en mí y hacen de nuestro centro de labores un lugar de conocimiento constante.

A todos los amigos y compañeros que contribuyeron en la finalización de este trabajo.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADÉMICO-PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE UN MODELO SIMPLIFICADO DE FIRMA DIGITAL BASADO EN TECNOLOGÍA PKI Y LA INVOCACIÓN POR PROTOCOLOS CASO DE ESTUDIO: MUNICIPALIDAD DE MIRAFLORES

Autor:	AGUILAR ALCARRÁZ, Gino Brehan
Asesor:	DE LA CRUZ VÉLEZ DE VILLA, Percy Edwin
Título:	Para optar el Título de Ingeniero de Sistemas
Fecha:	Noviembre 2015

RESUMEN

La seguridad de la información de cualquier organización pública o privada sufre constantemente ataques informáticos provenientes de terceros, incluso desde los usuarios internos que pretenden alterar o comprometer uno de los recursos más valiosos, la información. Por ello, es muy importante emplear un mecanismo certero y robusto, pero a la vez fácil de implementar que permita asegurar la integridad, autenticidad y confidencialidad los datos que residen dentro de una organización sin que se pueda repudiar o negar su autoría.

La tecnología de la firma digital permite garantizar la integridad de los datos y confiar de su procedencia, ya que si se produce una alteración de la información firmada, la firma digital muestra evidencia fehaciente que ha sido alterada o está corrompida y deja de ser íntegro.

Para dicho fin, la firma digital hace uso de un certificado digital, de confianza, que identifica inequívocamente a su poseedor en un mundo digital así como también de un par de llaves matemáticamente relacionadas. Dichos certificados residen en un contenedor criptográfico, el cual garantiza la seguridad y la correcta manipulación mediante aplicaciones de alto nivel que hacen uso del certificado digital.

En el presente trabajo, se implementará un modelo simplificado de firma digital que se soporta en las tecnologías de la PKI y la invocación por protocolos.

Con la adaptación de estas tecnologías, se podrá realizar la firma digital haciendo uso de aplicaciones web con total independencia del navegador, sistemas operativos, ActiveX o cualquier tecnología JAVA (applets, máquinas virtuales de JAVA), evitando así las configuraciones complicadas y dependencias de terceros.

Palabra clave: Firma digital, PKI, certificados digitales, independencia de JAVA, dispositivos criptográficos.

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA ACADÉMICO-PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTATION OF A SIMPLIFIED MODEL OF DIGITAL SIGNATURE BASED ON PKI TECHNOLOGY AND PROTOCOL INVOCATION
CASE OF STUDY: MIRAFLORES MUNICIPALITY

Author:	AGUILAR ALCARRÁZ, Gino Brehan
Advisor:	DE LA CRUZ VÉLEZ DE VILLA, Percy Edwin
Title:	Para optar el Título de Ingeniero de Sistemas
Date:	November 2015

ABSTRACT

Information security of any public and private organization faces frequently third party attacks, and even from theirs internal users who pretend to alter or compromise one of the most important valuable resources "**the information**".

Therefore, it is very important to use an certain and robust mechanism, but at the same time easy to implement that lets ensure the data integrity, authenticity and confidentiality that resides inside of the organizations without it can be repudiated or doubt of its authorship.

Digital signature ensure the date integrity and trust of their origin, because if a data is modified after the signature process, the own digital signature shows a real evidence that the data had been altered or is corrupted and does not keep full.

In order to get this works, digital signature uses a trusted digital certificate that identifies uniquely to its cardholder in a digital world as well as exits a key pairs mathematically related between them.

These certificates reside in a cryptographic device, which ensures the security and the proper manipulation by high-level applications using digital certificates.

In this work, I will implement a simplified digital signature model that is supported over PKI technology and protocols invocation.

With the mix of these technologies is possible make digital signature through web applications completely independence of any web browser, operating system, ActiveX plugin, extension or JAVA technology (applets, JVM), avoiding complicated configuration and third party dependence.

Keywords: Digital signature, PKI, digital certificate, independence of Java, cryptographic devices.

ÍNDICE DE CONTENIDOS

Pág.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE SIGLAS Y ABREVIATURAS

3DES	Triple Algoritmo de Cifrado de Datos
AAC	Autoridad Administrativa Competente
AC	Autoridad de Certificación
ACM	Asociación de los Sistemas Informáticos
AES	Estándar de Cifrado Avanzado
ANSI	Instituto Nacional Estadounidense de Estándares
API	Interfaz de programación de aplicaciones
AR	Autoridad de Registro
CAdES	Firma Electrónica Avanzada de CMS
CC	Common Criteria
CJ	Consejo de Judicatura
CODESI	Comisión para el Seguimiento y Evaluación del Plan de Desarrollo de la Sociedad de la Información en el Perú
CRL	Lista de Certificados Revocados
CSP	Proveedor de Servicios Criptográficos
DES	Estándar de Cifrado de Datos
DLE	Diccionario de Lengua Española
DNIe	Documento Nacional de Identificación electrónico
DNTICS	Dirección Nacional de Tecnologías de la Información y Comunicación
EEPROM	ROM programable y borrable eléctricamente
ETSI	Instituto Europeo de Normas de Telecomunicaciones
FIPS	Estándares Federales de Procesamiento de la Información
HSM	Módulo de Seguridad de Hardware
ICERT-EC	Entidad de Certificación del Consejo de la Judicatura
IDE	Entorno de Desarrollo Integrado
IEC	Comisión de Electrotecnia Internacional
IEEE	Instituto de Ingeniería Eléctrica y Electrónica
INACAL	Instituto Nacional de Calidad
INDECOPI	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
IOFE	Infraestructura Oficial de Firma Electrónica
JDK	Kit de Desarrollo de Java
NTP	Protocolo de Tiempo en red
ONGEI	Oficina Nacional de Gobierno Electrónico e Informática
PDF	Formato de Documento Portable
PAdES	Firma Electrónica Avanzada de PDF
PCM	Presidencia de Consejo de Ministros
PIN	Número Personal de Identificación
PKCS	Estándares Criptográficos de Llave Pública
PKI	Infraestructura de Llave Pública
RENIEC	Registro Nacional de Identificación y Estado Civil
RSA	Rivest, Shamir y Adleman
SHA	Algoritmo de Hash Seguro

SID	Sistema de Intermediación Digital
SSL	Capa de Puertos Seguros
SUNARP	Superintendencia Nacional de los Registro Públicos
TSA	Autoridad de Sellado de Tiempo
TSL	Lista de Proveedores de Confianza
tsp	Transacciones por segundo
UBL 2.0	Lenguaje Universal de Negocios
URI	Identificador de Recurso Uniforme
UTC	Tiempo Universal Coordinado
XAdES	Firma Electrónica Avanzada de XML
XML	Lenguaje de Marcas Extensible

CAPÍTULO I: PLANTEAMIENTO METODOLÓGICO

El rápido y constante avance de la tecnología ha conducido a significativas mejoras en el tiempo de respuesta de los servicios informáticos, la disponibilidad de los servicios web, la integridad de sistemas, así como a un procesamiento más preciso y detallado, con una mayor cantidad de información. De este modo, la enumeración de los diferentes beneficios que resultan de implementar tecnología en cada uno de los diferentes ámbitos, para el beneficio de la sociedad y del ciudadano, puede proseguir.

Más aun, la mayoría de procesos de las empresas y organismos del estado hoy en día están siendo trasladados o tercerizados siendo soportados dentro de sistemas de información mucho más robustos con más software especializado, que manejan grandes volúmenes de datos y obtienen respuestas en tiempo real. Esta es la manera en que la generación de información inmediata y procesada de manera correcta ayuda en la toma de decisiones.

La preocupación y el miedo de la mayoría de usuarios convencionales (no tecnológicos) gira alrededor de la seguridad de la información, y expertos en tecnología batallan día a día para poder garantizar la mayor seguridad y confiabilidad de la información procesada que es manipulada en sistemas informáticos, internet, una red local, un servidor FTP (Protocolo de Transferencia de Archivos, traducido del inglés *File Transfer Protocol*), etc. Por esta razón, se implementa constantemente buenas prácticas de seguridad de la información en frameworks, con la finalidad de prevenir y mitigar los ataques informáticos y, asimismo, crear cultura organizacional de seguridad de la información entre los usuarios internos, externos y proveedores.

Una gran cantidad de archivos digitales son enviados y/o compartidos desde y para diferentes servicios, utilizando protocolos de comunicación segura, ya sea vía correos electrónicos, servidores web, file systems, servidor samba, entre otros. En ese contexto, surge una pregunta que día a día se vuelve más recurrente: ¿quién otorga el valor legal y la integridad a un archivo digital?

Si bien existen los logs[1] generados por cada transferencia o transacción de datos exitosos o fallidos, estos archivos no presentan ningún valor legal probatorio, sino que, más bien, constituyen una prueba electrónica que puede ser manipulada por los mismos responsables de los Data Center (Centro de Datos) o por un tercero que no es de confianza, comprometiendo de este modo la integridad de los datos.

La firma digital es el único mecanismo electrónico al día de hoy soportado en la tecnología de la PKI que permite otorgar a cualquier archivo la integridad de los

[1] Registro de los sistemas de información o de cualquier programa informático.

datos firmados, la autenticidad de pertenencia del firmante y el no repudio [SUBRAMANYA, 2006].

1.1. ANTECEDENTES DEL PROBLEMA

En los últimos años, las empresas han realizado esfuerzos para crear soluciones soportadas en sistemas informáticos, que almacena el mayor volumen de datos e información representada en archivos electrónicos que luego son materializados o reproducidos en un soporte físico.

Parte de esta información es representada en medios y soportes físicos, entre los cuales el papel es el de uso más extensivo con más fácil manipulación. Si bien existen mecanismos físicos (sellos, estampas, rúbricas, hologramas, etc.) que dotan de valor legal, autenticidad y pertenencia de un documento físico a través de una vinculación de la rúbrica; no sucede lo mismo en el mundo digital, donde constantemente se puede alterar la información y no tener pleno control del trato que recibe cada documento hasta su impresión en papel.

Actualmente la mayoría de los documentos generados digitalmente no son ya impresos ni enviados a través de un medio físico de comunicación, sino, más bien, enviados por correos electrónicos, o siguen un ciclo de vida dentro de un sistema de trámite documentario, por ejemplo.

En el mundo físico, para manifestar nuestra voluntad debemos hacer uso de nuestra firma manuscrita, asociada a nosotros desde el momento en el que cumplimos la mayoría de edad y con la cual damos fe de lo que queremos expresar. En el mundo electrónico, sin embargo, no existía un equivalente que permitiera otorgar el valor legal a un documento.

La alternativa más sencilla y fácil de controlar fue la digitalización de la rúbrica en formato de una imagen (png, jpg, gif, etc.) que era incrustada en el documento, pero este objeto resultaba fácilmente manipulable por un tercero y no garantizaba la integridad del documento firmado ni mucho menos otorgaba el valor legal.

En el año 2000, el Congreso de la República aprobó la ley N° 27269 Ley de Firmas y Certificados Digitales, que expresa explícitamente lo siguiente: «La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad», [CONGRESO DE LA REPÚBLICA DEL PERÚ, 2001].

De este modo se brindaba un mecanismo electrónico para garantizar la legalidad con eficacia jurídica de un archivo firmado digitalmente y el no repudio del mismo.

Al día de hoy, la autoridad competente encargada de administrar y regular el uso de la tecnología de la PKI en el Perú es la IOFE. Dentro de la TSL se incorpora a los actores claves reconocidos y acreditados, que permiten la aplicación de la PKI en soluciones como firma digital, facturación electrónica, sistema de intermediación digital, por mencionar algunos.

Asimismo, RENIEC ha sido designada por ley como Autoridad de Registro y de Certificación del Estado Peruano.

1.2. DEFINICIÓN DEL PROBLEMA

Las empresas y entidades del estado, y entre ellas la Municipalidad de Miraflores carece de un modelo simplificado web de firma digital que permita ser integrado en el workflow de gestión de documentos digitales en formato PDF y que cumpla los siguientes requerimientos:

- El software de firma digital debe contar con la debida acreditación ante INDECOPI.
- Debe poder trabajar con los certificados digitales emitidos por RENIEC y contenidos en dispositivos criptográficos tales como token o smart cards definidos por las empresas.
- Brindar a los documentos un mecanismo de seguridad de la información, protegiendo de esta forma su autenticidad e integridad.

1.3. OBJETIVOS

1.3.1. Objetivo principal

Implementar un modelo simplificado de firma digital basado en tecnología PKI y la invocación por protocolos dentro de la Municipalidad de Miraflores.

1.3.2. Objetivos secundarios

- Evitar las dependencias de la tecnología Java, ActiveX o de cualquier aplicación de terceros para la implementación de la firma digital.

- Permitir la compatibilidad con cualquier navegador Web que soporte HTTP REST full[2].
- Permitir a los usuarios internos (gerentes y sub gerentes de la Municipalidad de Miraflores) realizar la firma digital haciendo uso de los certificados digitales emitidos por RENIEC.
- Realizar firma digital cumpliendo con las exigencias dispuestas en la Ley N° 27269, Ley de firmas y certificados digitales.
- Adaptar la firma digital haciendo uso de la tecnología PKI con software libre y la invocación por protocolos.
- Evitar la impresión de grandes volúmenes de documentos.

1.4. JUSTIFICACIÓN

La necesidad de la Municipalidad de Miraflores de emplear un mecanismo que permita otorgar a sus documentos digitales la integridad y confidencialidad ha conllevado la necesidad de implementar la firma digital dentro del workflow[3] interno.

Las razones fundamentales que dan origen al presente trabajo son:

La gran cantidad de papel demandada por las unidades organizativas de la Municipalidad de Miraflores las cuales son impresas y firmadas manualmente.

Estas unidades organizativas son: Procuraduría pública municipal, Órgano de Control Institucional, Administración documentaria y archivo, Secretaria general, Alcaldía, Registros Civiles, Trámite de separación convencional y divorcio ulterior, Huaca Pucllana Gerencias y Sub gerencias [MUNICIPALIDAD DE MIRAFLORES, 2015].

Tabla 1: Ranking del consumo de papel bond expresado en remesas de la Municipalidad de Miraflores- tercer trimestre 2015

Fuente: [MUNICIPALIDAD DE MIRAFLORES, 2015]

N°	CENTRO DE COSTO	JULIO	AGOSTO	SEPTIEMBRE	TOTAL
1	SUBGERENCIA DE RECAUDACIÓN	66	74	117	**257**
2	SUBGERENCIA DE REGISTRO Y ORIENTACIÓN TRIBUTARIA	50	70	60	**180**
3	GERENCIA DE ADMINISTRACIÓN TRIBUTARIA	43	45	68	**156**
4	SUBGERENCIA DE FISCALIZACIÓN Y CONTROL	29	30	70	**129**
5	SUBGERENCIA DE LICENCIAS DE EDIFICACIONES PRIVADAS	55	35	35	**125**

[2] Este protocolo permite el empleo de los métodos: GET, PUT, POST, DELETE.
[3] Es el flujo de documentos que se transmite basado en procedimiento.

6	SUBGERENCIA DE LOGÍSTICA Y CONTROL PATRIMONIAL	45	36	33	**114**
7	SUBGERENCIA DE RECURSOS HUMANOS	30	30	30	**90**
8	PROCURADURIA PUBLICA MUNICIPAL	15	30	35	**80**
9	SUBGERENCIA DE OBRAS PÚBLICAS	25	30	20	**75**
10	SUBGERENCIA DE CONTABILIDAD Y FINANZAS	0	20	40	**60**
11	SUBGERENCIA DE COMERCIALIZACIÓN	15	20	20	**55**
12	ÓRGANO DE CONTROL INSTITUCIONAL	8	15	25	**48**
13	ADMINISTRACION DOCUMENTARIA Y ARCHIVO	15	20	12	**47**
14	GERENCIA DE CULTURA Y TURISMO	13	7	16	**36**
15	SECRETARIA GENERAL	8	7	17	**32**
16	SUBGERENCIA DE CATASTRO	15	0	15	**30**
17	ALCALDÍA	0	12	14	**26**
18	REGISTROS CIVILES	10	12	4	**26**
19	SUBGERENCIA DE DEFENSA CIVIL	0	7	17	**24**
20	SUBGERENCIA DE FISCALIZACIÓN TRIBUTARIA	8	8	8	**24**
21	SUBGERENCIA DE MOVILIDAD URBANA Y SEGURIDAD VIAL	6	11	7	**24**
22	GERENCIA DE AUTORIZACIÓN Y CONTROL	0	10	10	**20**
23	GERENCIA MUNICIPAL	10	0	10	**20**
24	GERENCIA DE PARTICIPACION VECINAL	0	10	10	**20**
25	SUBGERENCIA DE LIMPIEZA PUBLICA Y ÁREAS VERDES	0	10	10	**20**
26	SUBGERENCIA DE PRESUPUESTO	0	8	10	**18**
27	SUBGERENCIA DE SERENAZGO	10	0	6	**16**
28	SUBGERENCIA DE SALUD Y BIENESTAR SOCIAL	0	0	15	**15**
29	GERENCIA DE ADMINISTRACIÓN Y FINANZAS	0	10	0	**10**
30	GERENCIA DE ASESORÍA JURÍDICA	0	10	0	**10**
31	GERENCIA DE PLANIFICACIÓN Y PRESUPUESTO	0	0	10	**10**
32	GERENCIA DE SEGURIDAD CIUDADANA	10	0	0	**10**
33	SUBGERENCIA DE DESARROLLO AMBIENTAL	0	8	0	**8**
34	SUBGERENCIA DE RACIONALIZACIÓN Y ESTADÍSTICA	0	8	0	**8**
35	TRAMITE DE SEPARACIÓN CONVENCIONAL Y DIVORCIO ULTERIOR	8	0	0	**8**
36	HUACA PUCLLANA	0	3	2	**5**
37	SUBGERENCIA DE DEPORTE Y RECREACIÓN	5	0	0	**5**
38	GERENCIA DE DESARROLLO URBANO Y MEDIO AMBIENTE	0	0	4	**4**
Total general (en resmas)[4]		499	596	750	**1,845**

Las vulnerabilidades a las cuales se expone una aplicación desarrollada en Java, la cual pone en riesgo la información transmitida dentro y fuera de una organización. Dicha vulnerabilidad, que permite atacar la confidencialidad e integridad de las comunicaciones, se debe a un error en una función del paquete AWT (Abstract Widget Toolkit), kit de herramientas de tratamiento de imágenes. El tipo de vulnerabilidad es CVE-2013-2463. [NIST, 2014].

[4] Las unidades están expresadas en resmas, cada resma contiene de 500 hojas.

Vulnerabilidad en el Java Security Manager, que permite obtener permisos para ejecutar comandos arbitrarios en el sistema operativo con Java 7. Un atacante podría utilizar técnicas de ingeniería social para hacer que usuarios visiten un enlace a un sitio web que aloje un applet malicioso. [US-CERT, 2013].

Según la Agenda Digital Peruana 2.0 [CODESI, 2011], se da cumplimiento con la Estrategia 1 «Impulsar la Interoperabilidad entre las instituciones del Estado para la cooperación, el desarrollo, la integración y la prestación de más y mejores servicios para la sociedad» y la Estrategia 3 «Desarrollar e implementar mecanismos para asegurar el acceso oportuno a la información y una participación ciudadana como medio para aportar a la gobernabilidad y transparencia de la gestión del Estado» dentro del Objetivo 7 «Promover una Administración Pública de Calidad orientada a población».

La consideración de que «el uso eficiente de las Tecnologías de la Información y la Comunicación (TIC) es un elemento transversal en la definición de políticas nacionales relacionadas con la gobernabilidad democrática, la transparencia y el desarrollo equitativo y sostenible» [ONGEI, 2013] es necesario para un gobierno abierto dentro del Perú.

En el siguiente gráfico se muestra cómo el Gobierno Electrónico es uno de los ejes transversales de una política de modernización que apoya el desarrollo de una gestión pública orientada a resultados y a favor del ciudadano. [PCM, 2013].

Figura 1: Pilares centrales de la Política de Modernización de la Gestión Pública

Fuente: [PCM, 2013]

La Ley 27269, Ley de Firma y Certificados Digitales y la Ley 27310 que regulan la utilización de la firma digital otorgándole la misma validez y eficacia jurídica que la firma manuscrita u otra análoga, estableciéndose los lineamientos generales respecto de los Prestadores de Servicios de Certificación Digital y la necesidad de contar con una Autoridad Administrativa Competente encargada de regular de manera más específica esta materia.

1.5. PROPUESTA DE TESIS

En el presente trabajo se realizará la implementación de un modelo simplificado de firma digital a través de la tecnología PKI e invocación por protocolos para el workflow web, haciendo uso de certificados digitales contenidos en tokens criptográficos de los gerentes y sub gerentes de Municipalidad de Miraflores.

Organigrama de la Municipalidad de Miraflores

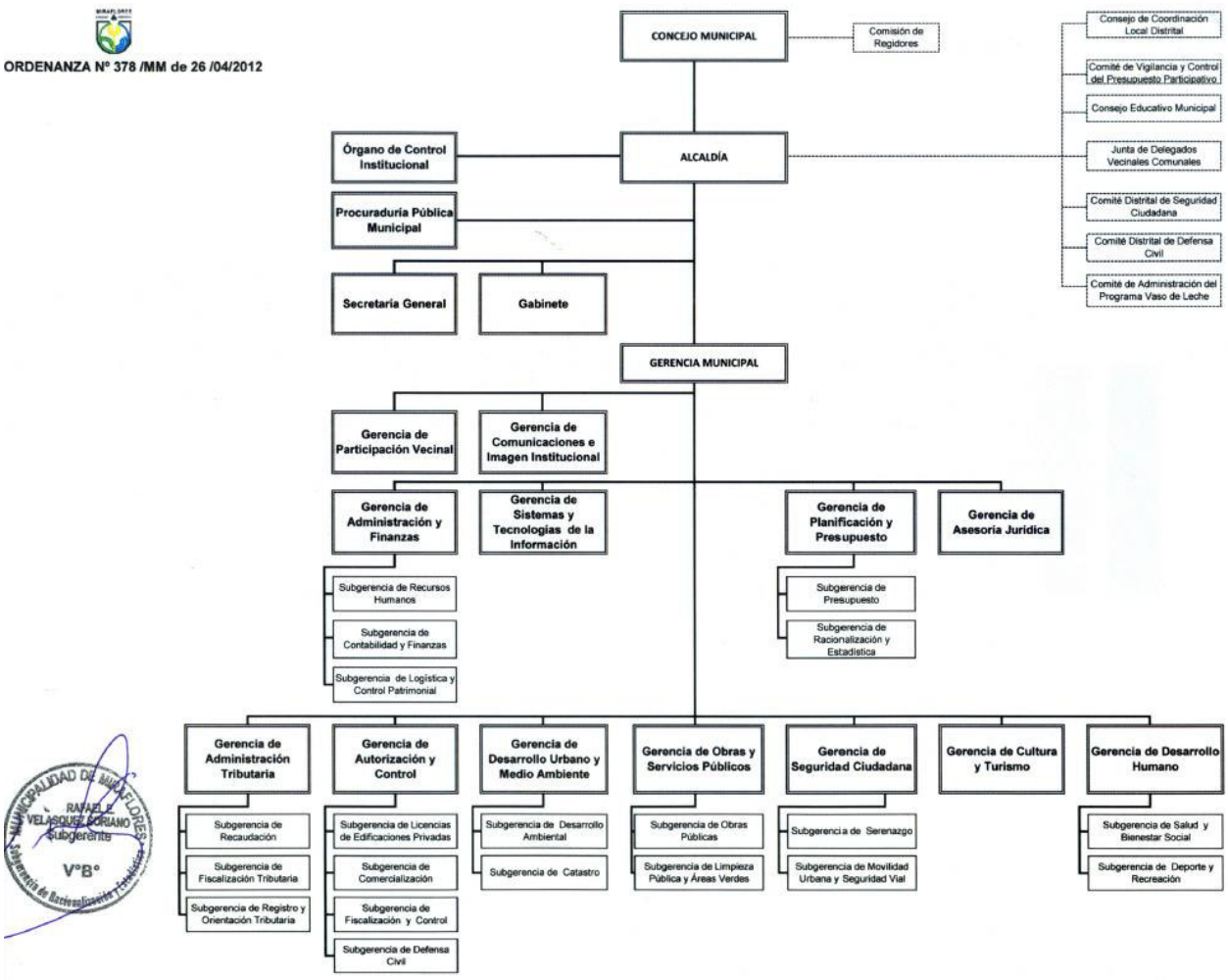


Figura 2: Organigrama de la Municipalidad de Miraflores

Fuente: [MUNICIPALIDAD DE MIRAFLORES, 2015]

Se muestra la organización jerárquica de todas las unidades que se encuentran dentro de la Municipalidad de Miraflores.

1.6. PRESENTACIÓN DEL RESTO DE LA TESIS

El presente trabajo está organizado en 7 capítulos:

- En el capítulo 2, correspondiente al Marco Teórico, se presenta una breve pero importante descripción de conceptos clave que servirá para el mejor entendimiento del presente trabajo.
- En el capítulo 3, correspondiente al Estado del Arte, se define los siguientes puntos: la taxonomía del problema, el marco legal que regula la utilización de la firma digital en el Perú, las diversas aplicaciones existentes en la actualidad basadas en la tecnología PKI, la revisión de la bibliografía y casos de éxitos; y se finaliza con un análisis Benchmarking entre, los algoritmos hash, algoritmos de firma digital, dispositivos criptográficos y soluciones Refirma, Xólido y 4identity.
- En el capítulo 4, correspondiente al Aporte Teórico, explica las diferentes tecnologías, algoritmos y programas que pueden servir para resolver el problema; y, adicionalmente, se explica la selección de las tecnologías que permitirán el cumplimiento del objetivo principal del presente trabajo.
- En el capítulo 5, correspondiente al Aporte Práctico, se muestra en qué tecnología se desplegará la solución, haciendo uso de la infraestructura que dispone la Municipalidad de Miraflores.
- En el capítulo 6, correspondiente a la Implementación, se desarrolla los diagramas de flujo y casos de uso; así como también se describirá la parte esencial del código web empleado para la solución del problema.
- En el capítulo 7, se dará a conocer las conclusiones obtenidas durante la elaboración del presente trabajo, así como también, los futuros trabajos relacionados con la firma digital dentro de la regulación Peruana.

CAPÍTULO II: MARCO TEÓRICO

En este capítulo se explicará detalladamente los conceptos clave y terminologías fundamentales que nos permitirán tener un mejor entendimiento y compresión del presente trabajo, obteniendo así el conocimiento adecuado de la teoría que lleva esta investigación.

2.1. INVOCACIÓN POR PROTOCOLOS

Es un funcionamiento universal que los sistemas operativos mantengan una serie de asociaciones entre tipos de archivos y las aplicaciones que son capaces de tratarlos. Así, si en un sistema operativo Windows se indica que se abra un documento de texto, este consultará en el Registro de Windows cuál es la aplicación por defecto asociada para su tratamiento (usualmente, el Bloc de Notas), y procederá a abrir esta aplicación pasando como parámetro la ruta completa del archivo en el esquema de argumentos definido en el propio Registro de Windows como parte de la asociación.

Este mecanismo de invocación por protocolo de los sistemas operativos es usualmente accesible desde los navegadores Web. Esto quiere decir que si en la barra de direcciones del navegador Web indicamos una URI, el navegador Web trasladará el control al sistema operativo para que este localice la aplicación apropiada para tratar el protocolo asociado a la URI, y la abra pasándole dicha URI [WEBPKI.ORG, 2015].

Como la invocación por protocolo no deja de ser una transferencia de datos desde una página Web (no necesariamente de confianza) a una aplicación nativa, los navegadores Web acostumbran a advertir de este cambio al usuario. En general, todos los navegadores Web muestran algún tipo de advertencia, excepto Apple Safari en Windows, OS X e iOS y WebKit (Android).

2.2. TECNOLOGÍA PKI

Es una combinación de elementos hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

Una infraestructura de llaves públicas es un sistema de entrega de certificados y llaves criptográficas, lo cual posibilita la seguridad en transacciones económicas financieras y el intercambio de información sensible entre personas relativamente desconocidas [ONGEI, 2002].

En la siguiente figura se muestra los procesos básicos de los elementos de un sistema PKI convencional.

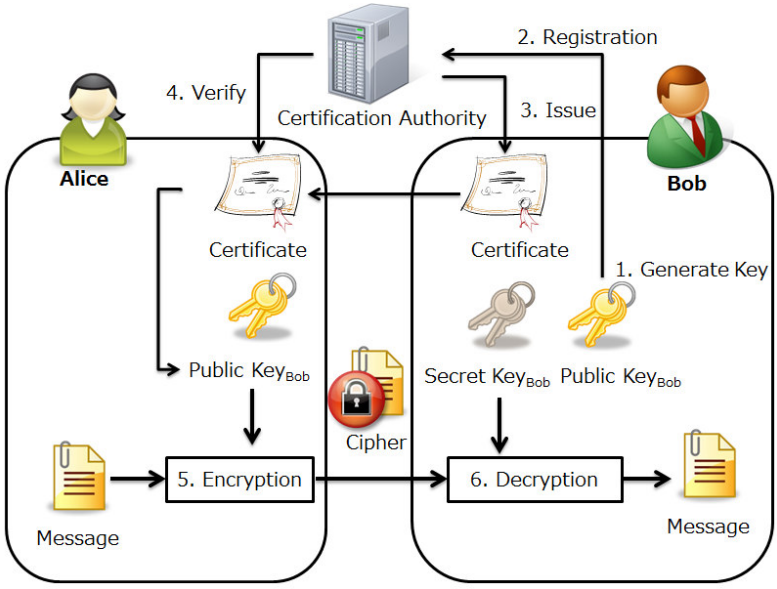


Figura 3: Infraestructura PKI
Fuente: [CIPHER, 2012]

En el Perú, la Autoridad Administrativa Competente de la Infraestructura Oficial de Firma Electrónica es INDECOPI (Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual).

Fundamentalmente, en una Arquitectura de PKI las principales entidades son:

- Una Autoridad de Certificación (CA) que controla el ciclo de vida de los certificados digitales
- Autoridades de Registro (RA) que identifiquen a los usuarios y los cuales se les entrega su respetivo certificado digital
- Suscriptores o usuarios de los certificados
- Repositorios que almacenen los certificados y la lista de certificado revocados (CRL).

Seguidamente en la Figura 4 se visualizan las Autoridades básicas y necesarios que interactúan en un sistema PKI, y adicionalmente el usuario final.

Figura 4: Entidades de una PKI

Fuente: [CÁNOVAS, 2002]

2.3. ESTÁNDAR PKCS

Las Normas de criptografía de clave pública son especificaciones elaboradas por los laboratorios de la RSA en cooperación con los desarrolladores de sistemas seguros en todo el mundo, con el propósito de acelerar el despliegue de la criptografía de clave pública. Publican por primera vez en 1991 como resultado de reuniones con un pequeño grupo de los primeros en adoptar la tecnología de clave pública, los documentos PKCS han sido ampliamente referenciados e implementados. Asimismo, las contribuciones de las series PKCS se han convertido en parte de muchas de las normas formales. Entre las más importantes contribuciones están los documentos ANSI X9, PKIX, SET, S/MIME y SSL [RSA, 2015].

A través de los siguientes estándares PKCS, es posible realizar la implementación de firma digital web para la Municipalidad de Miraflores; los demás estándares no serán mencionados, ya que no son requeridos para el presente trabajo.

2.3.1. PKCS #1

Este estándar define el tipo de cifrado RSA. Es un sistema criptográfico de clave pública desarrollado por Rivest, Shamir y Adleman. En honor a ellos se colocó las primeras letras de sus apellidos para darle nombre a este algoritmo. [RSA, 2015].

2.3.2. PKCS #3

Este estándar describe un método para la implementación del acuerdo de claves Diffie-Hellman. La aplicación prevista de este estándar permite el establecimiento de comunicaciones seguras.

2.3.3. PKCS #10

Este estándar se refiere a la solicitud o petición de firma de certificado, o CSR, según sus siglas en inglés. Esta solicitud es enviada a una Autoridad de Certificación para que pueda ser firmada y reconocida dentro de la jerarquía de la clave pública de la AC.

2.3.4. PKCS #11

Este estándar define el API genérico para que se pueda acceder a la información y, sobre todo, al certificado contenido en un dispositivo criptográfico. [RSA, 2015].

Cada proveedor de dispositivo criptográfico provee de las librerías, o middleware, para interactuar. La extensión de estas librerías sigue la extensión de .dll [NCRYPTOKI, 2014].

Cada proveedor de dispositivos criptográficos gestiona un middleware propietario.

2.3.5. PKCS #12

En él se define un formato de archivo con extensión .p12 o .pfx que contiene una clave privada con su respectivo certificado de clave pública, protegiéndolo a través de una clave simétrica.

Dichos archivos pueden ser instalados en un sistema operativo, en sus respectivos contenedores de confianza, tales como:

- Windows: Cryptographic Application Programming Interface (CAPI).
- Linux: Almacén central.
- MAC OX: Llavero.
- Mozilla: Network Security Services (NSS).

Esta práctica no se recomienda, ya que se puede tener tantas identidades digitales como instalaciones de los certificados, sin la posibilidad de tener un control riguroso.

Las buenas prácticas sugieren la custodia de certificados digitales dentro de dispositivos criptográficos (token, smart cards o HSM) que cumplan con las certificaciones internacionales de seguridad. Esto permitirá asociar una identidad digital a un contenedor seguro y el usuario tendrá un control absoluto del mismo [INDECOPI, 2008].

2.4. FUNCIÓN HASH

Una función hash H es una transformación que tiene una entrada m y devuelve una cadena de tamaño fijo, que se llama el valor hash h (es decir, h = H (m)). Las funciones hash con apenas esta propiedad tienen una variedad de usos computacionales generales. Sin embargo, cuando se las emplea en la criptografía, las funciones hash suelen ser elegidas para tener algunas propiedades adicionales [RSA, 2015].

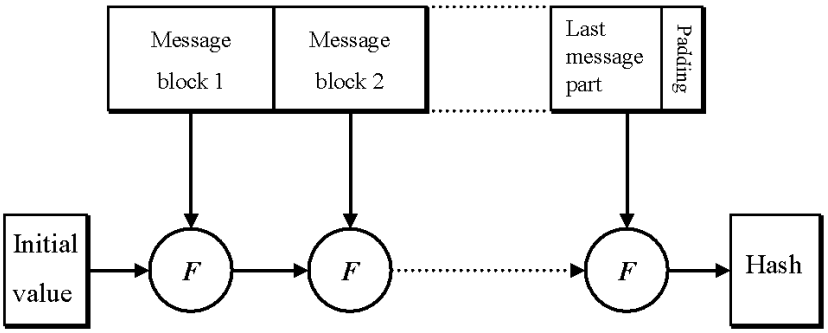


Figura 5: Estructura iterativa para funciones Hash

Fuente: [DAMGARD, 1990]

2.5. CRIPTOGRAFÍA

Tradicionalmente, el ámbito de la criptología ha sido concebido como el que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes, con el fin de hacerlos ininteligibles a receptores no autorizados. Estas técnicas se utilizan tanto en el arte como en la ciencia. Por tanto, el único objetivo de la criptografía era conseguir la confidencialidad de los mensajes. Para ello se diseñaba sistemas de cifrado y códigos. En esos tiempos, la única criptografía existente era la llamada criptografía clásica, definida como el arte de escribir con clave secreta o de un modo enigmático, según el DLE.

2.5.1. Objetivo

Su finalidad es poder garantizar el secreto de la información enviada por el emisor hacia un receptor y que este sea el único capaz de poder obtener la información tal cual el emisor la ha enviado, sin sufrir la más mínima alteración en el proceso.

2.5.2. Tipos

2.5.2.1. Criptografía Simétrica

También llamada criptografía de clave privada o criptografía de una clave, es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a ella, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y este lo descifra con la misma clave. [GARCÍA, 2008]

Uno de los principales inconvenientes con este tipo de sistema no está ligado a su seguridad, sino al intercambio de claves. El canal utilizado para el intercambio debe ser lo suficientemente seguro. Una vez que el remitente y el destinatario hayan intercambiado las claves, pueden usarlas para comunicarse con seguridad.

Dado que toda la seguridad se centra en la clave, esta tiene que ser difícil de adivinar. Esto quiere decir que el abanico de claves posibles, es decir, el espacio de posibilidades de claves, debe ser amplio. Algunos algoritmos vigentes a fecha de la presentación de este trabajo son: DES, 3DES, AES y Blowfish.

A continuación se muestra como una misma llave compartida se utiliza para encritpar y desencriptar un mensaje.

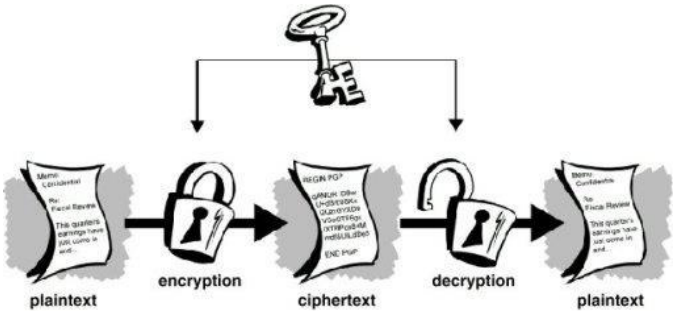


Figura 6: Criptografía Simétrica

Fuente: [GARCÍA, 2008]

La robustez de este tipo de cifrado se sustenta en el uso de estas dos técnicas:

Transposición o permutación: Es el intercambio de las posiciones de las letras de un texto en claro siguiendo un

cierto patrón. El mensaje cifrado contiene las mismas letras del mensaje pero en posiciones diferentes, lo que impide una fácil lectura.

Sustitución: Consiste en que los caracteres de un mensaje permanezcan en sus posiciones originales, pero sustituidos por otras letras, números o símbolos, siguiendo un patrón definido.

Este método de cifrado no es recomendado al día de hoy, pues a través del criptoanálisis se ha venido realizando estudios de los sistemas criptográficos con el fin de encontrarle debilidades y romper su seguridad sin saber la clave secreta compartida [INTYPEDIA, 2010].

Los ataques de fuerza bruta han permitido vulnerar los algoritmos de cifrado simétrico, ya que este ataque define el procedimiento según el cual, haciendo uso de un algoritmo de cifrado conocido y de un par de texto claro -> texto cifrado, se realiza operaciones de cifrado y descifrado, respectivamente, para poder encontrar las posibles combinaciones de clave.

2.5.2.2. Criptografía Asimétrica

Este tipo de criptografía utiliza un par de claves (clave pública y clave privada) para el envío del mensaje: una para cifrar y otra para descifrar el mensaje. Lo que se cifra en emisión con una clave, se descifra en recepción con la clave pública. [GARCÍA, 2008]

Las claves pública y privada son otorgadas por la autoridad de certificación. Aunque ambas claves son propias de cada persona, la clave privada no se transmite nunca y se mantiene secreta. La clave pública, por el contrario, se puede y se debe poner a disposición de cualquiera, pues fue creada con esa finalidad. Esto no implica ningún problema de seguridad, dado que es imposible deducir la clave privada a partir de la pública.

Se puede cifrar un mensaje con la clave pública y descifrar con la privada, dando confidencialidad al mensaje, ya que solo podrá ser visto por el usuario con la correspondiente clave privada.

De igual manera, se puede cifrar con la clave privada y descifrar con la pública, de modo que se consigue el no repudio al mensaje y que el firmante sea el autor fidedigno.

En la siguiente figura se visualiza como la llave privada es utilizada para realizar el encriptado del mensaje y la llave pública se utiliza para descifrar del mismo previamente cofrado.

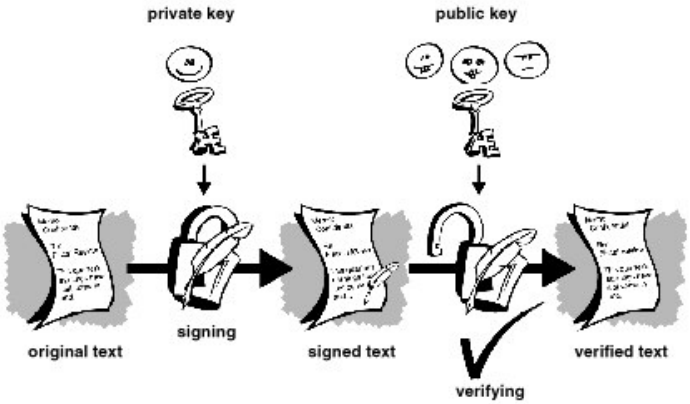


Figura 7: Criptografía Asimétrica

Fuente: [GARCÍA, 2008]

La ventaja de este tipo de criptografía es que no se comparte la clave privada y los demás participantes pueden verificar el contenido con la misma clave pública.

El más extendido de los sistemas de clave pública es el RSA, que fue desarrollado por Rivest, Shamir y Adleman, y es conocido como criptosistema RSA. Este algoritmo es reversible; es decir, además de permitir cifrar con la clave pública y descifrar con la privada, permite cifrar con la clave privada y descifrar con la clave pública.

2.5.2.3. Criptografía Híbrida

Este tipo de criptografía utiliza tanto el cifrado simétrico como el asimétrico. Emplea el cifrado de clave pública para compartir una clave para el cifrado simétrico. El mensaje que se envía en el momento se cifra usando la clave única (cifrado asimétrico) y se envía al destinatario.

2.6. ESTÁNDAR X.509

Es parte de la serie X de los estándares internacionales propuestos por la ISO (International Organization for Standarization) y la ITU (Internacional Telecommunication Union). Los estándares X.500 se

diseñaron para proporcionar servicios de directorio a grandes redes de computadoras, mientras que el X.509 proporcionó el marco para autenticar los mencionados servicios.

El formato de los certificados X.509 ha evolucionado en tres versiones a lo largo de los años: el X.509 v1, diseñado en 1988, certificaba las claves públicas de entidades que tenían asociado de forma única un nombre x.500; el X.509 v2, propuesto en 1993, proporcionaba más identificadores para asociar los certificados a una entidad; y, finalmente, el X.509 v3, publicado en 1997, mejoró la flexibilidad de su versión predecesora implementando un mecanismo genérico para añadir extensiones.

2.6.1. Certificados X.509 V3

Es un documento electrónico emitido por una Entidad de Certificación (EC). El certificado digital vincula la identidad física de una persona con su identidad digital. Con la identidad digital es posible ejecutar acciones de comercio y gobierno electrónico con seguridad, confianza y pleno valor legal [RENIEC, 2015].

Se trata de un documento electrónico que, generado y firmado digitalmente por una entidad de certificación, vincula un par de claves con una persona natural o jurídica confirmando su identidad [INDECOPI, 2007].

Un certificado digital es un documento electrónico que permite identificar a su poseedor en un mundo digital de manera inequívoca y para dicho fin existen parámetros establecidos en donde se alimentan con los valores personales de identificación del poseedor del certificado tal como se muestra en la siguiente figura.

version	version number; an integer, value is "2" for version 3	
serial number	unique identifier for each certificate generated by issuer; integer	
signature algorithm ID	algorithm identifier	algorithm used to sign certificate
	parameters	should not be used
issuer name	name of issuer (X.500 "distinguished name" that uniquely identifies a directory object),	
validity period	notBefore	Time
	notAfter	Time
subject name	name of subject (X.500 "distinguished name")	
subject public key info	algorithm identifier	subject's signature algorithm
	parameters	parameters applicable to subj. pub. key
	public key	subject's public key
issuer unique identifier	(optional) contains additional information about the subject; certificate must be version 2 or higher - not used by the Federal PKI.	
subject unique identifier	(optional) contains additional information about the issuer; certificate must be version 2 or higher - not used by the Federal PKI.	
extensions	(optional)	
issuer's signature	algorithm identifier	algorithm used for this signature
	parameters	should not be used
	ENCRYPTED (certificate hash)	

Figura 8: Certificado X.509 V3

Fuente: [NIST, 1998]

Los campos del certificado se explican a continuación:

- **Versión:** Versión del certificado (v3).
- **Serial number:** Identificador único del certificado, otorgado por la CA.
- **Signature algorithm ID:** Identificador del algoritmo de firma con el cual se firmó el certificado.
- **Issuer name:** Nombre de la entidad emisora.
- **Validity period:** Periodo de validez del certificado.
- **Subject name:** Nombre distinguido del nombre de la persona del certificado referido.
- **Subject public key:** El valor de la clave (en hexadecimal) pública de la entidad y el algoritmo con el cual debe usarse esa clave.
- **Issuer unique identifier:** Secuencia de bits que permite identificar unívocamente a la entidad emisora.
- **Subject unique identifier:** Secuencia de bits que permite identificar unívocamente a la entidad receptora.
- **Extenions:** Opcional
- **Issuer's signature:** Es el valor criptográfico obtenido a partir del resumen hash del certificado y la clave privada de la entidad emisora.

2.6.2. Declaración de Prácticas de Certificación (CPS)

Es un documento propio de cada CA en el que se declara y establece un conjunto de compromisos que adquiere la entidad respecto a las prácticas para la gestión del ciclo de vida de los certificados digitales que emite, así como un conjunto de medidas de seguridad del entorno. Este documento es en sí un compromiso adquirido, al que se referencia en todos los certificados emitidos en un campo establecido a tal efecto. [FIRMAPROFESIONAL, 2016]

2.6.3. Políticas de certificación (CP)

Se trata también de un conjunto de compromisos adquiridos por la CA con los usuarios de sus certificados, aunque, en este caso, este documento únicamente hace referencia a un tipo concreto de certificados dentro de la jerarquía. Por tanto, la Política de Certificación únicamente afecta a una tipología concreta de

certificado de CA Subordinada. Este mecanismo le facilita a la CA la capacidad de establecer unas directivas de certificación global y común mediante la Declaración de Prácticas de Certificación, así como la posibilidad de establecer requisitos concretos para tipos de certificado concreto cuando proceda. [FIRMAPROFESIONAL, 2016]

Es importante destacar que en ningún caso la implementación de Políticas de Certificación es una obligación, por lo que se deja a elección de la CA su implementación en base a sus requisitos y necesidades.

2.6.4. Obtención de un Certificado Digital

El proceso que se describe a continuación se refiere a cómo una persona puede solicitar su identidad digital (certificado digital).

1. El solicitante se dirige ante la RA, en donde deberá presentar la documentación e información para identificar físicamente al individuo. Cada RA es libre de solicitar la documentación suficiente.
2. La RA se encarga de validar la documentación y la información del solicitante. En algunos casos se debe realizar el pago por el trámite administrativo y el concepto de certificado digital.
3. Se envía la solicitud ante una CA, que firmará la solicitud y, en respuesta, devolverá un certificado digital firmado con los datos del solicitante y la información de la CA .según el estándar X.509 v3. (Ver apartado 2.6.1.)

2.6.5. Ciclo de vida de un Certificado Digital

Esta sección abarca todas las operaciones de gestión de la información contenidas en los certificados (par de claves, extensiones, identificadores, periodo de validez, datos sobre la entidad emisora, etc.) y realizadas por distintas entidades que componen la PKI.

- **Emisión:** El usuario final debe apersonaste ante al AR y el operador de identificación reconoce al usuario verificando los datos a ser emitidos en el certificado. Luego el operador de emisión de la AC genera el certificado. Mientras el certificado se encuentre en el periodo de validez.
- **Suspensión:** Este estado es opcional y depende de las CPS y el caso de uso a emplear. A través de algún autoservicio, el usuario solicita a la RA la suspensión de su

certificado. Una vez suspendido, este deja de tener validez aunque no haya expirado su tiempo de vida. Si el usuario no presenta los motivos de la suspensión del certificado, este se revoca automáticamente.

- **Reactivación:** Esta operación está permitida siempre y cuando el certificado no se encuentre revocado y esté suspendido. Mediante su aplicación, el certificado vuelve a ser válido.
- **Revocación:** Cuando un certificado vence, su tiempo de vigencia es automáticamente revocado. En algunos casos, cuando la clave privada es comprometida, el usuario puede solicitar ante la RA la revocación automática del mismo o puede hacerlo a través de un autoservicio implementado en la misma RA. Luego de cada revocación de un certificado, este pasa a pertenecer a la CRL, en donde se va actualizando a razón de 24 horas y se apila cada certificado revocado.
- **Renovación:** La renovación consiste en una nueva emisión del certificado digital.

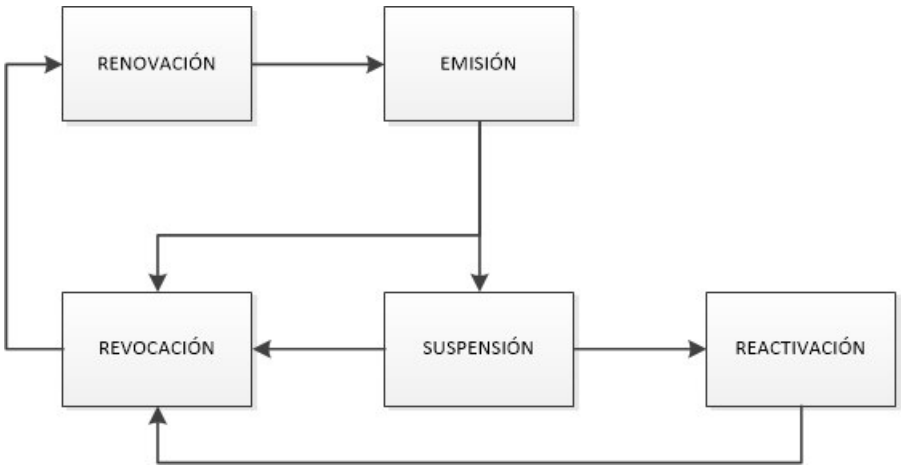


Figura 9: Ciclo de vida de un Certificado

Fuente: [Elaboración propia]

En la figura anterior se muestra las diferentes etapas del ciclo de vida de un certificado digital.

2.7. OID

El OID (Object Identifier), o Identificador de Objetos definen los campos o parámetros a partir de los cuales se alimentarán para generar un

certificado digital y para acceder a los campos de la CRL, siguiendo las políticas de certificación de una CA. [CÁNOVAS, 2002]

Cada CA puede variar sus políticas de seguridad y por ende sus OIDs respectivos. A continuación se muestra los OIDs de una CA federal.

Extension	Used By	Use	Critical (see Note)
Key and Policy Information			
authorityKeyIdentifier	all	identifies the CA key used to sign this certificate	No
keyIdentifier	all	unique with respect to authority.	
authorityCertIssuer	all	identifies issuing authority of CA's certificate; alternative to key identifier	
authorityCertSerialNumber	all	used with authorityCertIssuer	
subjectKeyIdentifier	all	identifies different keys for same subject	No
keyUsage	all	defines allowed purposes for use of key (e.g., digital signature, key agreement...)	Yes*
privateKeyUsagePeriod	all	for digital signature keys only. Signatures on documents that purport to be dated outside the period are invalid.	Opt.
certificatePolicies	all	policy identifiers and qualifiers that identify and qualify the policies that apply to the certificate	Opt.
policyIdentifiers	all	the OID of a policy.	
policyQualifiers	all	more information about the policy	
policyMappings	CA	indicates equivalent policies	No
Certificate Subject and Issuer Attributes			
subjectAltName	all	used to list alternative names (e.g., rfc822 name, X.400 address, IP address,...)	Opt.
issuerAltName	all	used to list alternative names	Opt.
subjectDirectoryAttributes	all	lists any desired attributes	Opt.
Certification Path Constraints			
basicConstraints	all	constraints on subject's role & path lengths	Yes*
cA	all	distinguish CA from end-entity cert.	
pathLenConstraint	CA	number of CAs that may follow in cert. path; 0 indicates that CA may only issue end-entity certs.	
nameConstraints	CA	limits subsequent CA cert. Name space.	Yes*
permittedSubtrees		names outside indicate subtrees are disallowed	
excludedSubtrees		indicates disallowed subtrees	
policyConstraints	all	constrains certs. issued by subsequent CAs	Yes*
policySet	all	those policies to which constraints apply	
requireExplicitPolicy	all	All certs. following in the cert. path must contain an acceptable policy identifier	
inhibitPolicyMapping	all	prevent policy mapping in following certs.	
CRL Identification			
cRLDistributionPoints	all	mechanism to divide long CRL into shorter lists	Opt.
distributionPoint	all	location from which CRL can be obtained	
reasons	all	reasons for cert. inclusion in CRL	
cRLIssuer	all	name of component that issues CRL.	

Figura 10: X.509 Standard Extensions and the FPKI

Fuente: [NIST, 1998]

Dentro de las políticas de certificación de una Autoridad de Certificación (CA), se selecciona los OID que serán parte de los atributos de los parámetros de un certificado.

En la columna Critical de la tabla anterior, se muestra los siguientes valores:

- **Yes:** Significa que el estándar permite que los campos sean tanto críticos o no críticos. Pero en la práctica se recomienda que sean críticos.
- **No:** El estándar solicita que la extensión sea no crítica si es usada.
- **Opt:** Significa que la CA emisora de certificados pueda escoger en hacer la extensión tanto crítica como no critica.

2.8. AUTORIDAD DE CERTIFICACIÓN (CA)

Persona jurídica pública o privada que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación. [INDECOPI, 2007].

Es la entidad principal del sistema, encargada de tramitar todas las solicitudes relacionadas al ciclo de vida de los certificados. No es posible acceder a ella de manera directa, sino a través de otros elementos intermedios confiables (como el servidor de solicitudes). Periódicamente, emite certificados digitales asociados a solicitudes pendientes, firma la lista de certificados revocados (CRL) y las políticas de certificación, y publica la información generada en los repositorios de datos tanto internos como externos. [CÁNOVAS, 2002]

Existen jerarquías de CA dentro de una PKI. La CA raíz se firma así miasma para garantizar la confianza en ella y luego firma a otras CA subordinadas que confían en la raíz; a esa acción se la conoce como confianza heredada. Los certificados digitales siguen la misma analogía, son firmados por CA subordinadas de confianza.

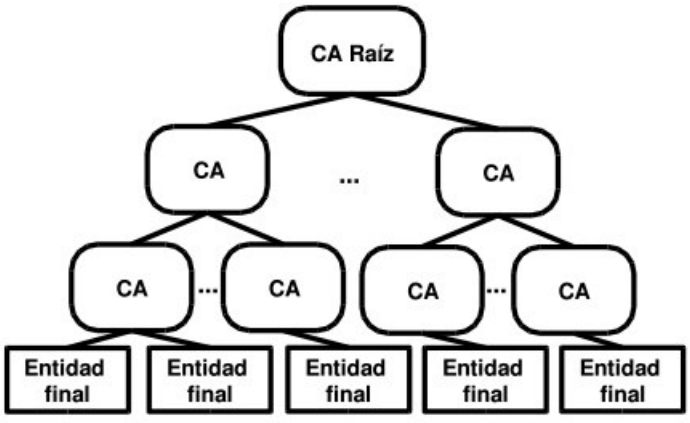


Figura 11: Modelo de confianza jerárquico

Fuente: [CÁNOVAS, 2002]

En una arquitectura PKI, cuando se genera el certificado raíz de una CA, esta queda offline por un periodo determinado de seis meses o un año por cuestiones de seguridad.

Se trata de una autoridad acreditada con la certificación Web Trust para emitir certificados digitales con valor legal, identificando al portador. Es la autoridad a la que el suscriptor solicita una identidad digital o certificado digital [WEBTRUST, 2011].

2.9. AUTORIDAD DE VALIDACIÓN (VA)

Es el ente facultado para suministrar la información sobre la vigencia de los certificados digitales emitidos por las CAs registrados en su RA correspondiente. Realiza esta acción a través de dos protocolos de validación actualmente soportados.

Los protocolos empleados por VA son:

- **CRL**: Lista de Certificados Revocados.
- **OCSP**: Protocolo de Estado de Certificados en Línea.

2.10. AUTORIDAD DE REGISTRO (RA)

Normalmente es la primera entidad de contacto con la infraestructura de certificación. Se trata de un software que, gestionado por un operador humano, se encargará de realizar todas las validaciones pertinentes que exija cada operación ejecutada. En líneas generales, la función principal de la RA es la de *identificación* y *validación* de las solicitudes de cualquier tipo. Para realizar sus funciones, toma en consideración las opciones determinadas por la política de certificación del sistema [CÁNOVAS, 2002].

Con excepción de los notarios públicos, es una persona jurídica encargada del levantamiento de datos, comprobación de estos respecto a un solicitante de un mecanismo de firma electrónica o certificación digital, la aceptación y autorización de las solicitudes para la emisión de un mecanismo de firma electrónica o certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de mecanismos de firma electrónica o certificados digitales. Las personas encargadas de ejercer la citada función serán supervisadas y reguladas por la normatividad vigente [INDECOPI, 2007].

La función de las Autoridades de Registro es controlar la generación de certificados para los miembros de una entidad. Previa identificación, la

Autoridad de Registro se encarga de realizar la petición del certificado y de guardar los datos pertinentes.

2.11. CRL

Es a veces necesario revocar certificados, por ejemplo, cuando el titular del certificado deja la organización emisora o cuando se vea comprometida la clave privada. El mecanismo definido en X.509 para revocar certificados es la lista de revocación de certificados (CRL).

Es una lista, firmada por la CA, de los certificados no vencidos, revocados. Una CRL contiene el tiempo de emisión, y puede contener el tiempo esperado en que la próxima CRL será publicada. Por otro lado, el usuario puede determinar si una copia de la CRL es aún vigente.

La Lista de Certificados Revocados permite realizar una validación rápida a través de una lista proporcionada por la CA que puede ser descargada desde el portal de la autoridad de certificación e internamente tiene una estructura parecida al de la siguiente figura.

Extension	Use	Critical
authorityKeyIdentifier	identifies the CA key used to sign CRL.	No
keyIdentifier	unique key identifier; alternative to **certIssuer** & **authorityCertSerialNumber**	
certIssuer	name of CA's cert. issuer	
authorityCertSerialNumber	used with **certIssuer**; combination must be unique	
issuerAltName	alternate name of CRL issuer	No*
cRLNumber	sequence number for CRL	No
issuingDistributionPoint	name of CRL distribution point; also gives reasons for revocations contained in CRL.	Yes
deltaCRLIndicator	indicates delta CRL (lists certificates revoked since last full CRL) & gives sequence number	Yes

Figura 12: Resumen de las extensiones de la CRL

Fuente: [NIST, 1998]

2.12. OCSP

Como suplemento de la comprobación periódica de la CRL, puede ser necesaria la obtención de información oportuna concerniente al estado de revocación de certificados.

El Protocolo de Estado de Certificados en Línea (OCSP) permite que las aplicaciones puedan determinar en tiempo real el estado de revocación de uno o más certificados al mismo tiempo, así como puede ser usado también para obtener información adicional del estado.

Un cliente OCSP envía una solicitud de estado para la aceptación de un respondedor o servidor OCSP y suspende la aceptación de los certificados en cuestión hasta que el respondedor proporcione una respuesta vía HTTP [IETF, 2013].

2.12.1. Solicitud OCSP

Una solicitud OCSP contiene la siguiente información:

- Versión del protocolo.
- Solicitud de servicio.
- Identificador de certificado objetivo.
- Extensiones opcionales, que pueden ser procesadas por el respondedor OCSP.

2.12.2. Respuesta OCSP

Todas las respuestas OCSP deberían estar firmadas digitalmente por una CA.

- Una respuesta definitiva está compuesta por:
- Versión de la sintaxis de respuesta.
- Identificador del respondedor.
- Tiempo en el que la respuesta fue generada.
- Respuestas para cada uno de los certificados en una solicitud.
- Extensiones opcionales.
- OID del algoritmo de firma.
- Firma calculada a través de una función hash de la respuesta.

Esta especificación define el siguiente indicador de respuesta definitiva para el uso del valor del estado del certificado:

- **Bueno:** Indica una respuesta positiva a la consulta del estado.
- **Revocado:** Indica que el certificado ha sido revocado.
- **Desconocido:** Indica que el respondedor no conoce acerca de la solicitud de certificado.

2.13. PSC

Los Proveedores o Prestadores de Servicios de Certificación son las personas físicas o jurídicas que expiden certificados digitales o prestan algún tipo de servicio en relación con la firma digital.

La principal función de una PSC es la de emitir certificados digitales con valor legal.

Para el Perú, una empresa que quiera convertirse en PCS debe pasar una acreditación que INDECOPI dispone para confiar en ella [INDECOPI, 2007].

Al día de hoy, se puede incorporar a una CA dentro de la TSL basándose en los decretos supremos [EL PERUANO, 2011], [EL PERUANO, 2012] y resolución Nº 45 de la CNB.

Una vez completada la acreditación, INDECOPI procederá a incorporar a esta empresa dentro de la TSL (Lista de Servicios de Confianza).

2.14. TSL

Es la lista que incorpora a los PSC de confianza que han pasado un riguroso proceso de acreditación. INDECOPI es la autoridad Administrativa Competente encargada de gestionar y dar mantenimiento a esta TSL.

A través de este mecanismo, la TSL permite la interoperabilidad entre los documentos firmados digitalmente y las comunicaciones seguras haciendo uso de certificados digitales de los PSC.

La TSL permite un control y dominio sobre los actores claves en materia de certificación digital con los cuales se impulsará el gobierno digital, comercio electrónico y el intercambio de información de confianza a través de medios digitales entre personas naturales y jurídicas.

La TSL de Perú se puede visualizar y descargar desde el siguiente link:

https://www.INDECOPI.gob.pe/web/firmas-digitales/lista-de-servicios-de-confianza-trusted-services-list-tsl-

2.15. CSP

El Proveedor de Servicios Criptográficos es una librería software que implementa el Microsoft CryptoAPI (API). El principal propósito del CSP es el de codificar y decodificar funciones que los programas puedan usar, como autenticación fuerte, firma digital o email seguro.

Es una especie de la capa intermedia (o middleware) por la cual una aplicación de alto nivel en Windows puede realizar operaciones criptográficas en un chip.

2.16. DISPOSITIVOS CRIPTOGRÁFICOS

Son dispositivos hardware que llevan un chip criptográfico que cumple el estándar ISO/IEC 7816 e ISO/IEC 7810.

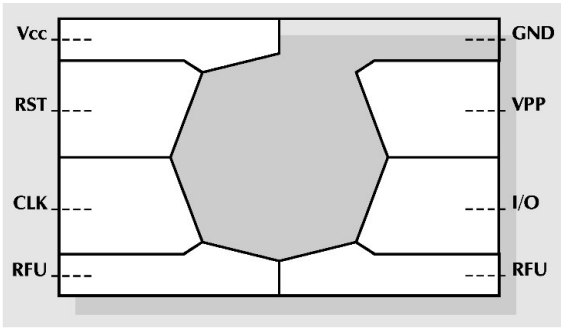


Figura 13: Chip Criptográfico

Fuente: [SMARTCARD.CO.UK, 2015]

En la figura se muestra el esqueleto de comunicación para realizar las operaciones criptográficas en la misma lógica del chip.

Estos dispositivos criptográficos pueden ser:

2.16.1. Smart card (tarjeta inteligente)

Es un dispositivo de las dimensiones de una tarjeta bancaria que contiene un procesador criptográfico seguro y cuenta con circuitos integrados que permiten la ejecución de cierta lógica programada [RENIEC, 2015].

También conocidos como tarjetas inteligentes, son del tamaño de una tarjeta de crédito convencional (ISO/IEC 7816 ID-1) o de tamaño SIM (ISO/IEC 7816 ID-000). Este chip lleva un micro CPU con el cual permite realizar operaciones criptográficas.

Para poder leer la información que lleva el chip, es necesario contar con un smart card reader (lector de tarjetas inteligentes) y tener instalado el middleware del proveedor del chip, de modo que este sea reconocido por el Sistema Operativo del usuario.

Para poder garantizar el uso adecuado del certificado que reside en el chip, se solicitará el ingreso del PIN; de no ingresarlo correctamente, se irán acabando los intentos. Generalmente, los chips incorporan un mecanismo de bloqueo (3 intentos) por cuestiones de seguridad.

Estos chips deben estar certificados con alguna de estas 2 certificaciones internacionales de seguridad:

- FIPS 140-2[5]
- Common Criteria EAL 4+[6]

Para el Estado Peruano, el Documento Nacional de Identidad Electrónico (DNIe) permite identificar a su poseedor tanto física como digitalmente.

El DNIe contiene un chip criptográfico con certificación Common Criteria EAL5 y sistema operativo que implementa las especificaciones de JavaCard 2.2.2 y Global Platform 2.1.1. Almacena en su memoria EEPROM datos del ciudadano en formato OACI, certificados digitales y datos biométricos. El chip y el sistema operativo cuentan con la certificación FIPS 140-2 Nivel 3 [RENIEC, 2015]. En la siguiente figura se detalla otros aspectos de seguridad física del DNIe.

Figura 14: DNIe
Fuente: [RENIEC, 2015]

2.16.2. Token criptográfico

Es un dispositivo criptográfico más versátil, ya que es un lector de chip criptográficos e incorpora el chip criptográfico, todo en un único dispositivo con conexión USB 2.0 tipo A.

Estos tokens deben estar certificados con: FIPS 140-2 y/o CC EAL 4+.

Algunos tokens emplean mecanismos o sistemas adicionales, como tamper proof (ante cualquier intento malintencionado, el token dejará evidencia) o tamper resistant (ante cualquier uso malintencionado, el chip se dañará y quedará inservible).

[5] Ver Anexo.
[6] Ver Anexo

2.16.3. HSM (Hardware Security Module)

Es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y aporta aceleración hardware para operaciones criptográficas (tps). Estos dispositivos pueden tener conectividad SCSI / IP u otras y aportar funcionalidad criptográfica de clave pública (PKI) de alto rendimiento que se efectúa dentro del propio hardware.

2.17. SELLADO DE TIEMPO

La finalidad de un sellado de tiempo es garantizar que un determinado evento ha sido realizado en un determinado instante en el tiempo y que estos no han sido modificados. Para que un sello de tiempo pueda considerarse de confianza, la estructura de datos que lo contiene debe estar protegida criptográficamente y la marca de tiempo debe haber sido obtenida de una fuente tercera confiable.

Empleando la utilización de proveedores de valores basados en UTC (Universal Time Coordinated) y un servicio NTP (Network Time Protocol) de confianza, se puede asegurar el tiempo y hora en cada instante.

El resellado se aplica antes de que el certificado de la TSA caduque y se pueda prolongar la validez temporal de la firma.

2.17.1. NTP

Es un protocolo de Internet que permite sincronizar relojes entre sistemas informáticos a través de enrutamientos de paquetes de red. Está diseñado para resistir latencias variables utilizando el puerto 123.

El servidor NTP de confianza en el Perú está disponible en el INACAL y hay que pedir su registro a través de este link: http://www.inacal.gob.pe/inacal/index.php/servicios-metrologia/que-es-la-hora-nacional?id=483

2.17.2. UTC

Es el principal estándar internacional que regula el tiempo en el mundo. Se emplea a través de relojes atómicos.

2.17.3. TSA (AUTORIDAD DE SELLADO DE TIEMPO)

Una Autoridad de Sellado de Tiempo firma un mensaje (resumen) con el fin de probar que existía antes de un determinado tiempo.

Los pasos para solicitar un sellado de tiempo son:

- Un usuario solicita ante una TSA la obtención de un sello de tiempo para un documento electrónico que él posee.
- Un resumen digital (técnicamente, un hash) se genera para el documento en el ordenador del usuario.
- Este resumen forma la solicitud que se envía a la TSA.
- La TSA genera un sello de tiempo con esta huella, la fecha y hora obtenidas de una fuente fiable, y las firma digitalmente.
- El sello de tiempo se envía como respuesta al usuario.
- La TSA mantiene un registro de los sellos emitidos para su futura verificación.

2.18. FIRMA DIGITAL

La firma digital es equivalente a la firma manuscrita y permite sustituirla para todos los efectos legales.

La firma digital proporciona seguridad para las transacciones electrónicas haciendo uso de una clave privada y clave pública; también proporciona confidencialidad, autenticidad y el no repudio, a los documentos electrónicos firmados de esta manera. [GAIKWAD, 2015]

Es un valor criptográfico obtenido a partir del resumen digital del certificado y la clave privada de la entidad emisora [CÁNOVAS, 2002].

Una firma digital es un mecanismo criptográfico que permite al destinatario de un mensaje firmado digitalmente determinar la entidad de confianza de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado.

La firma digital se aplica en aquellas áreas donde es importante poder verificar la autenticidad y la integridad de ciertos datos, por ejemplo, documentos electrónicos o software, ya que proporciona una herramienta para detectar la falsificación y la manipulación del contenido.

2.18.1. Tipos de Firma Digital

Dependiendo de las necesidades del usuario, este puede aplicar los siguientes tipos de firma:

- **Firma Simple:** Firmas básicas que solo contiene la firma de un único firmante.
- **Co-Firma:** También conocida por soportar múltiples firmas en un mismo nivel de jerarquía. Para este caso, no importa el orden en el cual se aplica la firma digital; lo importante es que se cuente con todas las firmas requeridas. Se la emplea en documentos de reunión, conferencias, comités, etc [SANS, 2015].
- **Contra Firma:** En este caso, el orden de la firma múltiple es importante. Un documento que sigue un flujo normal en el que se necesita que diversos firmantes apliquen su firma, cada uno de estos deberá refrendar la firma del predecesor.

2.19. FORMATOS DE FIRMA DIGITAL

Según las necesidades y escenarios específicos, se aplica diversos formatos de firmas digitales para los diferentes tipos de archivos.

2.19.1. CAdES (CMS avanzado)

Es el formato binario de firma usado para la encriptación, autenticación, resumen y firma de documentos. Este formato de firma esta soportado en el estándar PKCS#7.

Una vez firmado este archivo, no es posible realizar la verificación y visualización con un programa específico, ya que la información se guarda de forma binaria, teniendo un esquema como el de la siguiente figura.

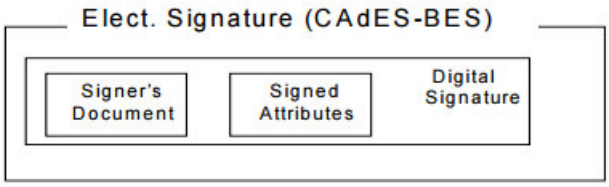


Figura 15: Ilustración de firma digital CadES – BES

Fuente: [ETSI, 2012]

2.19.2. PAdES (PDF avanzado)

Es el formato de uso más frecuente para cualquier aplicación que quiera firmas archivos PDF, ya que un PDF firmado "aparentemente" no sufre ninguna alteración del contenido y para los usuarios es fácil poder realizar las validaciones respectivas.

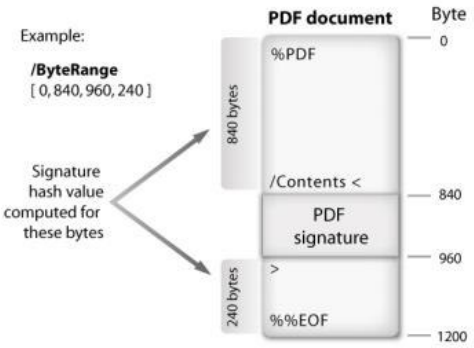


Figura 16: Estructura lógica de un archivo PDF firmado digitalmente

Fuente: [ETSI, 2009]

En la Figura 16 se muestra los Bytes que son firmados y embebidos posteriormente dentro del mismo documento sin alterar la información original.

Dentro del mismo estándar es posible que sea soportada la firma gráfica tal como se muestra en la siguiente figura.

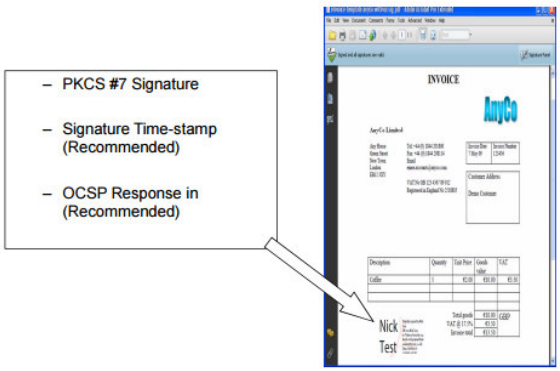


Figura 17: Firma digital en formato PAdES –BES

Fuente: [ETSI, 2009]

2.19.3. XAdES (XML avanzado)

Es una especificación desarrollada bajo el amparo del w3c que permite la firma (completa o parcial) de documentos utilizando una notación XML estándar. El formato XAdES ofrece algunas ventajas frente a la firma tradicional, puesto que al estar basado en texto plano, su estructura es legible por humanos.

Funciona de igual manera que el formato CAdES, pero es más extensible y está orientada a documentos XML.

Una firma XML que se utiliza para firmar un recurso fuera del documento XML que la contiene es denominada como una firma separada (detached). Si se utiliza para firmar la firma parcial de un documento que la contiene, es llamada firma envuelta (enveloped). Si contiene los datos firmados dentro de sí mismo, es llamada firma envolvente (enveloping), y en la siguiente figura se aprecia la etiqueta <ds:Signnature ID?> que es donde se contiene la firma digital.

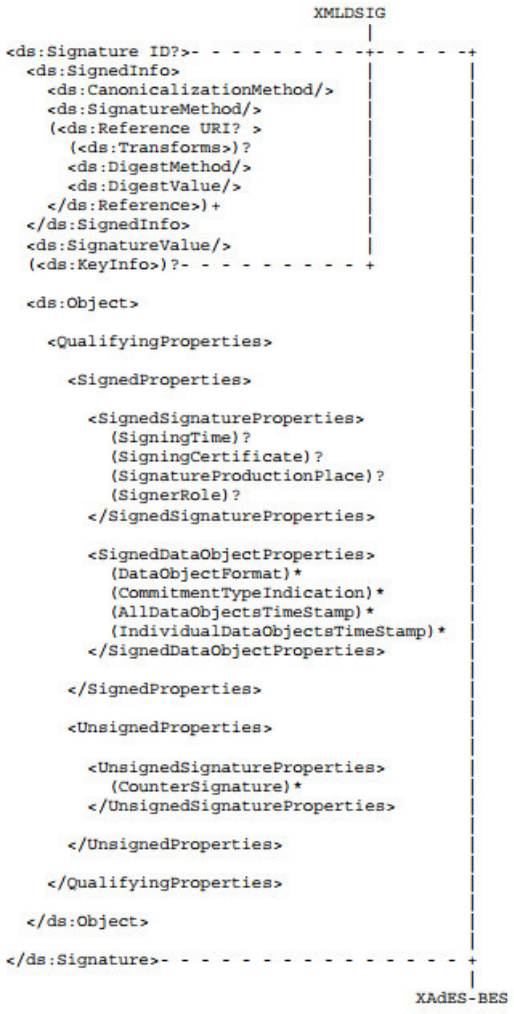


Figura 18: Estructura lógica de firma digital XAdES –BES

Fuente: [ETSI, 2010]

Para los formatos de firma CAdES, PAdES y XAdES, existen variaciones que importa mencionar:

-BES: Es el formato básico para satisfacer los requisitos de la firma electrónica avanzada.

-T: Se añade un sellado de tiempo al documento firmado.

-C: Se añade un conjunto de referencias a los certificados de la cadena de certificación y a su estado de revocación, como base para una verificación longeva.

-X: Se añade sellos de tiempo a las referencias creadas en el paso anterior.

-XL: Se añade los certificados y la información de revocación de los mismos, para su validación a largo plazo.

-A: Permite la adición de sellos de tiempo periódicos para garantizar la integridad de la firma archivada o guardada para futuras verificaciones.

2.20. VENTAJAS DE LA FIRMA DIGITAL

Entre los beneficios más representativos de la firma digital, podemos mencionar los siguientes:

- Permite la integridad de un documento, ya que un archivo firmado digitalmente no puede ser modificado sin dejar un rastro o huella.
- Permite dotar a la firma de una duración de muchos años, así como de una posibilidad de validación en cualquier instante de tiempo.
- Los tiempos de entrega y envío de documentos firmados se reducen considerablemente dentro de una organización.
- Permite garantizar la autoría del documento, evitando así el repudio del documento firmado.
- Permite firmar lotes considerables de documento digitales, los cuales, si fueran llevados al mundo físico, demandarían mucho más tiempo y cansancio.
- La indexación de los documentos firmados es más fácil, puesto que puede ser manipulada por un software de gestión de documentos sin necesidad de complicadas integraciones.
- Garantía legal y respaldo jurídico, ya que la firma digital tiene el mismo valor que una firma manuscrita.

CAPÍTULO III: ESTADO DEL ARTE

3.1. TAXONOMÍA

Debido a su naturaleza, el presente trabajo puede ser clasificado dentro de las diferentes líneas de investigación de las instituciones tecnológicas de la ACM, IEEE y de la UNMSM.

- Según la clasificación taxonómica que proporciona la ACM, el presente trabajo se ubica en la siguiente sección: “Applied Computing SIGAPP”.
- Según la clasificación taxonómica que proporciona la IEEE, el presente trabajo se ubica en la siguiente sección: “IEEE Systems, Man & Cybernetics Society”.
- Según el “Programas y Líneas de Investigación en la Universidad Nacional Mayor de San Marcos”, publicado el 10 de Setiembre del 2014 por el Vicerrectorado de Investigación, el presente trabajo se ubica en la siguiente sección:

  AREA C: INGENIERÍAS

  C.0.3. TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

  C.0.3.25. Tecnología de información y aplicaciones de sistemas

3.2. MARCO LEGAL y NORMATIVO

A continuación, se hace referencia a los documentos que son el aval jurídico para el desarrollo de la tecnología PKI en el Perú:

- Ley N° 27269 – Ley de Firmas y Certificados Digitales.
- Ley N°27310 – Ley que modifica el artículo 11 de la Ley N°27269.
- Ley N°27291 – Ley que permite el uso de medios electrónicos para la manifestación de voluntad y la utilización de la firma electrónica.
- Decreto Supremo N°052-2008-PCM – Reglamento de la Ley de Firmas y Certificados Digitales.
- Decreto Supremo N° 070-2011-PCM – Decreto Supremo que modifica el Reglamento de la Ley N°27269, Ley de Firmas Certificados Digitales y establece normas aplicables al procedimientos registral en virtud del Decreto Legislativo N°681 y ampliatorias.

- Decreto Supremo N°105-2012-PCM- Establecen disposiciones para facilitar la puesta en marcha de la firma digital y modifican el Decreto Supremo N°052-2008-PCM – Reglamento de la Ley de Firmas y Certificados Digitales.

3.3. APLICACIONES

Entre las aplicaciones que se basan en la tecnología PKI y certificados digitales, podemos mencionar las siguientes:

3.3.1. Firma Digital

Es aquella firma electrónica que cumple con todas las funciones de la firma manuscrita. En particular se trata de aquella firma electrónica basada en la tecnología de criptografía asimétrica. La firma digital permite la identificación del firmante, la integridad del contenido y tiene la misma validez que el uso de una firma manuscrita. La firma digital está vinculada únicamente al firmante.

A pesar que el proceso de firma digital varía según cada software que se use, se han considerado los pasos generales que se siguen para este proceso.

Una vez se tenga listo el documento electrónico que deseo firmar, acudo al "software de firma digital" y selecciono el documento que deseo firmar así como el certificado digital correspondiente, que también debe tener la capacidad de firmar documentos electrónicos. Se debe seguir con el procedimiento de firma digital que depende de cada software y que solicitará su contraseña de acceso a la clave privada de su certificado digital a fin de confirmar la acción de firma digital. Una vez culminado este proceso, el software incluirá la firma digital en el documento.

Cabe precisar que la "firma digital" no es un elemento visible como la firma manuscrita que podemos observar en el documento físico. Sin embargo, algunos softwares con la finalidad de brindar mayor confianza y seguridad al usuario incluyen un elemento visor con fines estéticos, una vez que el proceso de firma digital ha concluido satisfactoriamente.

3.3.2. Facturación Electrónica

La Factura Electrónica es un documento tributario en formato digital, que está a disposición de todos los contribuyentes. Este documento permitirá a las empresas realizar transacciones de emisión/recepción de comprobantes de pago, mejorando el modo de operación actual (emisión en papel pre-foliado), lo que reducirá

sustancialmente los costos administrativos y mejorará los procesos de las empresas.

El estándar en el cual se presenta la información de la factura es el formato XML (UBL 2.0), que es un tipo de XML especial que contiene datos del contribuyente y la firma digital embebida.

Entre los beneficios tangibles, podemos mencionar:

- Reducción de Costos Administrativo.
- Agilidad en la Operación Administrativa.
- Incremento en la Productividad.
- Seguridad en su Intercambio Electrónico.
- Impacto Ambiental.

3.3.3. Historias Clínicas Electrónicas

La historia clínica electrónica supone incorporar las Tecnologías de la Información y la Comunicación (TIC) en el núcleo de la actividad sanitaria. Esto trae como consecuencia que la historia deje de ser un registro de la información generada en la relación entre un paciente y un profesional de la salud o un centro sanitario, para formar parte de un sistema integrado de información clínica.

La historia clínica electrónica es el registro unificado y personal, multimedia, en el que se archiva en soporte electrónico toda la información referente al paciente y a su atención. Es accesible, con las limitaciones apropiadas, en todos los casos en los que se precisa asistencia clínica (urgencias, atención primaria, especialidades, ingresos hospitalarios y demás).

Debe integrarse toda la información multimedia que se utiliza en la práctica clínica. Almacenar adecuadamente esta información, hacerla amigablemente accesible, difundirla de forma adecuada a los posibles usos y con las garantías debidas (consentimiento, confidencialidad, seguridad y demás requisitos), y recibirla y reutilizarla en la forma más conveniente, es un proceso todavía en potencia.

Hay problemas de conceptualización del proceso de atención y del de implementación de las TIC, ya que no se ha demostrado que impacten positivamente en la calidad de la atención clínica, ni en la morbilidad, ni en la mortalidad. Además, hay problemas respecto a la codificación, las normas y los estándares.

3.3.4. Desmaterialización

Es el proceso por medio del cual un documento de papel es transformado en un documento electrónico. Hoy en día, se trata de una preocupación principal para las empresas y las administraciones. Percibida por lo general como la etapa relacionada con la digitalización, la desmaterialización cubre realmente diferentes campos estratégicos [SCRIBD, 2014].

Si nos preguntamos qué es desmaterializar, responderemos que es la transferencia de una información (textos, sonidos, imágenes) desde un soporte analógico (como el papel) hacia un soporte digital. La desmaterialización, asimismo, ofrece beneficios inmediatos. Dado que del 5 al 15% del volumen de negocios de una empresa se dedica a la gestión de sus documentos en papel, únicamente la impresión de páginas puede representar hasta el 3% del volumen de negocios de la empresa. Por ello, los beneficios de la desmaterialización son de tipo económico. Además, la desmaterialización con valor probatorio garantiza un mismo nivel probatorio entre el papel y los documentos electrónicos.

En la siguiente figura se visualiza gráficamente como es un proceso normal de desmaterialización.

Figura 19: Proceso de Digitalización
Fuente: [CYBERSEC, 2013]

3.3.5. Sistema de Intermediación Digital

Es un sistema automatizado que permite a SUNARP realizar digitalmente la constitución de empresas, evitando la presencia física de un notario dentro del proceso registral, la impresión de documentos, la falsificación documentaria y la comunicación inmediata a través del correo electrónico, todo esto en menos de veinticuatro horas [SUNARP, 2014].

URL del SID de SUNARP:
https://www.SUNARP.gob.pe/SintermediacionD.asp

Actualmente, este mecanismo se extiende para poder otorgar los diferentes tipos de poderes a las personas naturales sobre las personas jurídicas.

3.3.6. Voto electrónico

Es una expresión que comprende varios tipos de votación: abarca tanto los modos electrónicos de emitir votos (voto por internet) como los medios electrónicos de contar los votos.

Las tecnologías para el voto electrónico pueden incluir Smart cards, sistemas de votación mediante escáneres ópticos y quioscos de votación especializados (incluso sistemas de votación auto-contenidos, sistemas de votación de Registro o Grabación Electrónica Directa, DRE por sus siglas en inglés). También puede referirse a la transmisión de papeletas y votos por vía telefónica, redes privadas o por Internet.

Las tecnologías del voto electrónico pueden acelerar el conteo de los votos y proveer una mejor accesibilidad para los votantes con algún tipo de discapacidad. Sin embargo, ha sido calificado como anticonstitucional en algunos países (como Alemania) por no permitir la fiscalización del proceso por personas sin conocimientos altamente especializados.

Los sistemas de voto electrónico pueden ofrecer soluciones que permiten a los votantes verificar si sus votos han sido registrados y contados con cálculos matemáticos. Estos sistemas pueden aliviar preocupaciones respecto de votos registrados incorrectamente. Una forma de mitigar esas preocupaciones podría ser permitir a los votantes verificar cómo han votado, con algún tipo de recibo electrónico, firmado por la autoridad electoral mediante una firma digital. Esta característica podría probar en forma concluyente la exactitud del conteo, pero cualquier sistema

de verificación que no pueda garantizar la anonimidad de la elección del votante puede producir intimidación en el votante o permitir la venta del voto. Algunas soluciones criptográficas se dirigen a permitir al votante verificar su voto personalmente, pero no a un tercero. Una de las maneras sería proveer al votante de un recibo de su voto firmado digitalmente, así como también de recibos de otros votos seleccionados al azar. Esto permitiría que sólo el votante identifique su voto, pero no le permitiría probar su voto a nadie más. Además, cada voto podría estar señalado con una identificación de sesión generada al azar, lo que permitiría al votante verificar que el voto fue registrado correctamente en un control de auditoría público de la papeleta.

3.3.7. Autenticación fuerte

Cada vez que ingresa a su computador, lo más probable es que el sistema le solicite una clave de acceso para comprobar que efectivamente es usted el que está intentando acceder a su cuenta. Este tipo de autenticación se basa en algo que se sabe: la clave y algo que se tiene: un certificado digital.

No obstante, sabemos que por diferentes motivos otra persona puede tener esa clave y acceder al sistema de forma ajena; es entonces cuando hace presencia la Autenticación Fuerte.

La Autenticación Fuerte es una manera de asegurar que la persona que se identifica en un sistema es realmente quien dice ser. La comprobación de identidad que realiza este sistema se encuentra generalmente basada en tres factores fundamentales:

Algo que usted sabe: clave, PIN, Cédula de Identidad, Pasaporte, Nombre de Algún Pariente, etc.

Algo que usted posee: Credencial, Tarjeta Magnética, Token OTP (One Time Password), etc.

Algo que la persona es: Huella Digital, Reconocimiento facial, de voz, iris, retina, etc.

Hablamos de Autenticación Fuerte cuando un sistema utiliza al menos dos de los tres factores básicos, de modo que si uno de estos factores se encuentra comprometido, todavía existe un segundo factor que garantiza la seguridad.

La Banca, por ejemplo, utiliza sistemas de Autenticación Fuerte. En el momento en que usted visita un cajero automático para

retirar dinero, utiliza dos factores de autenticación: Algo que usted posee: su tarjeta, y algo que usted sabe: su clave.

3.3.8. Publicación certificada

A través de internet, día a día se coloca cantidades desmesuradas de información, en tal medida que no tenemos un conocimiento absoluto de si dicha información se encontraba presente en un tiempo inicial, de modo que luego, al querer acceder nuevamente, ya no es posible. Para resolver esto, la solución de publicación certificada es un mecanismo que permite garantizar de manera fehaciente que los datos e información han existido en un determinado momento de tiempo, y que tienen o no un tiempo de vigencia.

Este mecanismo es utilizado por las entidades del Estado para poder mostrar información pública a los ciudadanos; estos pueden consultarlo en un intervalo de tiempo apropiado. Asimismo, sirve también para las licitaciones, concursos, publicaciones, subastas, ofertas, etc.

3.4. REVISIÓN DE LA LITERATURA

3.4.1. Metodología de la Investigación

La información ofrecida y desarrollada en el presente trabajo ha sido recopilada, fundamentalmente, de papers/journals consultados a través de bases de datos indexadas, como: IEEE Xplore, ELSEVIER, International Journal of Computer Science and Mobile Computing (IJCSMC), Google Scholar, RSA. De igual modo, se consultó la información de entidades mundialmente reconocidas dedicadas a la investigación de la tecnología y su aplicación en mejora de la sociedad.

Criterios de selección

10 Artículos/papers/journals publicados:

- 01 artículo del 2014
- 01 artículo del 2013
- 02 artículos del 2012
- 01 artículos del 2011
- 02 artículo del 2009
- 02 artículos del 2008
- 01 artículo del 2005

Documentos oficiales de instituciones reconocidas internacionalmente tales como RSA, de modo que la procedencia de la información es confiable.

Información procedente de entidades de confianza.

Criterios de exclusión

- Artículos/papers/journals/tesis con una antigüedad mayor de 10 años.
- Información que aún se encuentre en la primera versión publicada.
- Información de entidades cuya información es dudosa o desconfiable.

Criterios especiales

También se considera los documentos oficiales que soportan y regulan la PKI del Estado Peruano, [INDECOPI, 2007], [INDECOPI, 2007A], [INDECOPI, 2008] e [INDECOPI, 2015].

A continuación, se explicará los aportes de diez papers consultados que han contribuido en la elaboración del presente trabajo.

3.4.2. Privacy Features of European eID Cards Specifications [NAUMANN, 2009]

Las tarjetas de identidad electrónica son la puerta para acceder a la información personal de su poseedor. La divulgación de la información privada es una violación de los derechos de privacidad de los ciudadanos.

El autor basa el paper en la comparación de las características de privacidad entre las tarjetas de identificación electrónica adoptadas en la Unión Europea.

Hace una comparación exhaustiva de las tecnologías vigentes empleadas en las identidades electrónicas europeas y el factor de las amenazas y los posibles delitos o ataques informáticos, lo cual conlleva a implementar mayores medidas de seguridad, pero sin complicar el uso de esta tecnología a los usuarios finales.

Al tratarse de un paper informativo, no emplea un proceso propio para resolver el problema; más bien, hace referencias a algunos estándares utilizados.

No menciona nada referente a las certificaciones FIPS140-2 o Common Criteria, certificaciones que garantizan un nivel de seguridad medio/alto al momento de utilizar la información contenida en los chips para realizar operaciones criptográficas.

La certificación europea, que respalda o asegura que la información almacenada en estos sea únicamente accedida por el doble factor de autenticación (“algo que tengo” y “algo que sé”), es Common Criteria.

Estas certificaciones acreditan que el software contenido en el hardware es seguro para realizar operaciones criptográficas.

El DNIe peruano utiliza un mismo PIN (clave de acceso) para realizar la autenticación fuerte y la firma digital, de modo muy parecido al estándar que siguen las tarjetas electrónicas de identificación de España.

La tecnología contactless (sin contacto) todavía presenta ciertas vulnerabilidades para poder garantizar la correcta trasmisión de los datos de los usuarios.

La sobreescritura o modificación de los datos personales es posible en algunos países de la unión europea, pero este es un tema polémico, ya que hay datos como el código fiscal, o algún servicio asociado, que no deberían poder ser cambiados tan fácilmente, sino bajo un respaldo jurídico o autorización del ente regulador de identidades electrónicas. Para dicho fin, se recomienda la reemisión de una identidad electrónica.

3.4.3. Secure Digital Signature Schemes Based on Hash Functions [NOROOZI, 2013]

El trabajo no realiza críticas puntuales a otros trabajos de tesis o papers presentados con anterioridad.

Hace hincapié en que únicamente con la aplicación de la tecnología PKI el intercambio de mensajes se daba de una manera segura sin el intercambio de claves.

Diffie and Hellman no emplearon una solución práctica para el uso de esta tecnología de llaves asimétrica sino hasta que Rivest, Shamir y Adlemen la utilizaron para desarrollar el paradigma de la firma digital.

Los autores hacen una comparación de los algoritmos Hash en diferentes aspectos, para los cuales se basan en algunos

indicadores estándares, y describen paso a paso la manera de realizar sus operaciones.

La firma digital se sustenta en el uso de funciones hash y el cifrado para garantizar la integridad y la autenticidad de la información firmada.

Existen algoritmos hash que ya han sido vulnerados y cuyo uso no es recomendable. La familia de SHA 2 es hasta ahora la más segura y robusta para garantizar la total seguridad en la firma digital. El algoritmo hash con mayor difusión en aplicaciones en el mercado es el SHA256.

Los autores hacen una comparación entre los mensajes hash versus mensajes hash cifrados o encriptados.

El proceso que los autores definen para generar un archivo hash sigue un algoritmo, según el cual a partir de un documento cualquier se genera una secuencia de caracteres que resume el documento electrónico. El algoritmo en cuestión es el siguiente:

```
int main (void) {

int x,y; int mn; strnset (sign, passlen*2);

FILE *myfile; char filename[80];

textmode(C80);

clrscr();

printf("Signature Generator Version 1.00\n");

printf("Enter File Name : ");

scanf("%s",filename);

myfile = fopen(filename,"rb");

if (myfile==NULL) { printf("\nCan not Open File %s !!!.\n",filename);

exit(0); } else {

hashing(myfile);

printf("\nHashing Was Compeleted ...\n");encoder();

printf("Result Was : %s\n",sign);fclose(myfile);

getch();getch();return0;};
```

Una vez obtenido el array de caracteres, se procede con la conversión de caracteres a Hexadecimal. Para tal fin, el autor sugiere el siguiente algoritmo para cifrarlo:

```
hi=data [i] &240

lo=data [1] & 15

int converttohex(char*data,char*result)

{int j=0; int i=0; int hi,lo;

  for (;i<passlen;i++)

    {hi=data[i] & 240;

     lo=data[i] & 15;

     hi=hi>>4;

if (hi>9)

    {hi=hi+'A"0'; };

if (lo>9)

{lo=lo+'A'-'9'-1; };

hi+='0';

lo+='0';

result [j++]=hi;

result [j++]=lo;

}; return 0;};
```

En la siguiente tabla se hace una comparación de los tamaños de Bytes generados por cada algoritmo de hash

Tabla 2: Comparación de tamaño de archivos en Bytes

Fuente: [NOROOZI, 2013]

SIZE OF ORIGINAL FILES (BYTE)	MD5 ALGORITHM (BYTE)	SHA1 ALGORITHM (BYTE)	SHA2 ALGORITHM (BYTE)
14	32	40	64
18	32	40	64
72	32	40	64

Tabla 3: Comparación de operaciones lógicas, estado actual y complejidad de hardware

Fuente: [NOROOZI, 2013]

ALGORITHM	LOGICAL OPERATION	CURRENT STATUS	HARDWARE COMPLEXITY
MD5 algorithm	AND,OR,NOT,Rotating shifts	Collision	Medium
SHA1 algorithm	AND,OR,NOT,Rotating shifts,XOR	Collision	Large-scale
SHA2algorithm	AND,OR,NOT,Rotating shifts,XOR	Running	Large

La tabla anterior muestra el estado actual de colisión de los algoritmos hash utilizados generalmente para firma digital, así como también la complejidad hardware que tienen para realizar las operaciones criptográficas.

No se ha mencionado nada al respecto de CCE (Criptografía de Curva Elíptica), que es una variante de criptografía asimétrica. Si bien no es un estándar aceptado internacionalmente, existen algoritmos para que puedan trabajar con claves más cortas y ser más rápidas en las operaciones, en comparación con los demás métodos.

Se irán creando más algoritmos en la medida que vayan siendo colisionados o vulnerados y comprometan la integridad de la información.

Los tamaños de archivos de hash son mucho menores (casi el 9% del tamaño original del archivo), lo que permite realizar una verificación más certera y rápida de los archivos.

La firma digital es la única manera de garantizar la autenticidad y la integridad de un documento electrónico.

3.4.4. Attacking Smart card system: Theory and practice [MARKANTONAKIS, 2009]

El autor ofrece una descripción general sobre los dispositivos criptográficos basados en smart cards o tarjetas inteligentes. El término es atribuido a una tarjeta cuando tiene memoria y posee la capacidad de realizar operaciones in situ a través de órdenes o instrucciones. En este caso, son órdenes que solo una smart card puede entender y manipular, y a las que solo una smart card puede devolver como resultado un valor específico.

Si bien una smart card es un dispositivo hardware, también involucra una parte de software precargado dentro de sí misma. Dependiendo de la naturaleza o la finalidad por la cual haya sido creada, las smart card pueden ser clasificadas en:

Memory card: Es una tarjeta simple que solamente lleva información precargada que se puede conectar a un sistema back-end. Por ejemplo, las tarjetas para control de accesos, tarjetas de prepago, etc.

Memory card with logic: Esta tarjeta, a diferencia de la anterior, contiene algo de lógica, según la cual realiza operaciones con la información precargada y puede ser modificada con ayuda de ciertas instrucciones. Las tarjetas del metropolitano, tarjetas de crédito o débito, etc., son muestras de este tipo.

Microprocessor cards: A diferencia de las anteriores, estas tarjetas llevan un microprocesador incorporado que les permite realizar operaciones criptográficas más avanzadas en comparación con las dos anteriores tarjetas. Adicionalmente, la memoria EEPROM (Memoria de solo lectura eléctricamente borrable y programable).

Contactless Smart card: A diferencia de las tres anteriores, estas tarjetas no son de contacto; es decir, para poder operar e intercambiar información no se necesita una interfaz física, sino, más bien, estar próximo a otro dispositivo que utilice la misma interfaz de no contacto. Las tarjetas más conocidas son las NFC, que necesitan un campo de proximidad no menor de diez centímetros.

Dual Interface cards: Este tipo de tarjetas utiliza una interfaz de contacto, así como también de no contacto, siendo, por tanto, un híbrido de ambas tecnologías.

En todos los casos, siempre existen ataques realizados por terceros que intentar vulnerar la seguridad y tener acceso a la información o al código secreto que almacena alguna de estas tarjetas, con lo cual se podría comprometer otra información valiosa. Existen diversas formas de ataque invasivo al hardware que poseen estas tarjetas; una de ellas es, por ejemplo, la manipulación del flujo de electricidad que se transmite en las tarjetas inteligentes con memoria, para así simular las ordenes autorizadas o enviadas por alguien de confianza.

Otro aspecto delicado es el tiempo en el cual se transmite estas peticiones. Al no poseer un time over o tiempo de finalización adecuado, deja un vacío en el cual un atacante podría intentar interceptar o enviar peticiones no autorizadas que simulen serlo.

Existen sistemas que se basan en el uso de smart card, como son los sistemas de TV por satélite, en los cuales cada smart card comparte una llave común que permite garantizar la confianza ante el agente de TV, mas no posee la capacidad de cifrar y descifrar la señal. En este caso, las tarjetas inteligentes cumplen el rol de dispositivos de tamper resistant o resistencia a la manipulación. El otro sistema muy conocido y usado por la mayoría es el EMV, que no es otra cosa que el sistema de pagos con tarjetas de crédito o débito haciendo uso de un terminal que posea la capacidad de leer la información de la tarjeta y trasmitirla al ente de confianza para que se autorice la transacción. En este caso, se simula que el poseedor de la tarjeta, un defraudador, obtiene el PIN de acceso de manera offline, sin que se envíe la petición a la autoridad emisora de la tarjetas, para que posteriormente se redirija la orden de pago por un monto mayor en cuanto el sistema se ponga on line. Para evitar este tipo de ataques, las tarjetas incluyen un sistema de terminales con tamper resistant.

En conclusión, el autor menciona que los productos smart card deben poseer al menos una certificación Common Criteria, garantía de seguridad, algoritmos seguros y protocolos que han sido sujetos a validaciones de expertos.

3.4.5. A Study of Electronic Document Security [PARAG, 2014]

Los problemas de seguridad de los documentos y la tecnología están cada vez más a la orden del día. A la fecha, suceden ataques de colisiones o de fuerza bruta que permiten encontrar vulnerabilidades en ciertos algoritmos, comprometiendo así el acceso a la información.

Cuando un emisor de información intenta enviar dicha información a un(os) destinatario(s) seleccionados previamente, siempre existe la duda de si en verdad el destinatario recibió lo que el emisor envió; más aún, si en el envío la información sufrió algún cambio intencionado o malintencionado.

Delitos como esto hacen que se implementen buenas prácticas y tecnología que permitan garantizar o asegurar el envío de información a través de canales no seguros, como internet.

Las organizaciones migran cada vez más sus servicios a un entorno telemático, donde la seguridad de la información puede verse comprometida.

Existen tres razones principales que cualquier entidad tiene que enfrentar cuando intenta compartir documentos electrónicos:

Requerimientos Regulatorios: Establecidos generalmente por el gobierno a través de leyes, o estándares internacionales ya adaptados y validados.

Retorno de la Inversión: La inversión tecnológica no debe ser vista como un gasto, sino como una medida de garantizar la continuidad del negocio.

Seguridad de la Información: La información como activo estratégico que aporta valor a la empresa.

El autor propone la persistencia en la seguridad de los documentos a partir de seis pilares: Confidencialidad, Autorización, Responsabilidad, Integridad, Autenticidad y el No Repudio. La siguiente figura muestra dichas características de cualquier documento firmado digitalmente.

Figura 20: Características de un documento firmado digitalmente

Fuente: [PARAG, 2014]

Con este esquema se puede controlar y asegurar que los documentos compartidos en cualquier tipo de red informática son

recibidos por los receptores autorizados y sin que el documento varíe.

El proceso para resolver el problema es hacer uso de la firma digital.

La firma digital garantiza la integridad, autenticidad y el no repudio de un documento electrónico firmado por un autor que quiere enviar cierta información a un destinatario y no quiere que dicho documento sea alterado de ninguna manera en el envío por medios electrónicos potencialmente inseguros o no controlados, ya que si bien se puede establecer una VPN (Virtual Private Networking, o Red Privada Virtual, en castellano), se estaría confiando en el canal de la información y no habría ningún rastro si el documento ha sido interceptado por un tercero y este lo ha modificado o leído a pesar de no tratarse de un destinatario valido.

Las aplicaciones más delicadas y con vigencia en el mercado son el envío de documentos y datos entre entidades gubernamentales, comercio electrónico, pago por internet, etc.

El proceso de firma digital consiste en lo siguiente:

- Crear un hash del documento original.
- La firma digital es creada, y esta cifra el hash con la clave privada del emisor.
- La firma digital es incluida con el documento.

El autor hace referencia a seis características fundamentales para garantizar la seguridad de documentos persistentes.

Lista las principales tecnologías utilizadas para asegurar estas seis características fundamentales que aseguran la seguridad de un documento. Estas se clasifican en:

Control de Documento:

- **Confidencialidad**: Basada en el cifrado.
- **Autorización:** Los privilegios soportados para modificar un documento.
- **Responsabilidad**: Puede rastrear el documento.

Firma Digital:

- **Integridad**: Permite que la verificación del documento original no haya sido modificada.

- **Autenticidad:** La pertenencia al autor del documento firmado.
- **No repudio**: Sirve para que el firmante no pueda negar un documento firmado con su clave privada.

Las imágenes empleadas no son de fácil lectura.

En las referencias bibliográficas cita las URL, pero no la fecha en las cuales han sido accedidas.

Usa como fuente de información Wikipedia.

No comenta sobre la firma longeva o de larga duración.

En la afirmación: «Electronic Acrobat supports multiple digital signatures placed anywhere in the document for proper presentation» [PARAG, 2014]. La firma digital o las firmas múltiples no pueden ser establecidas o mostradas en cualquier parte del documento para que pueda ser visible; la firma digital es el hash cifrado y firmado con la clave privada, y puede ser representada gráficamente por motivos estéticos.

En la medida en que las empresas vayan migrando sus datos sensibles a un soporte tecnológico o electrónico, esta información no debe ser alterada de ninguna forma.

Al crear más información digital, se deberá emplear mecanismos que aseguren la confidencialidad, contabilidad, integridad, autenticidad, el no repudio y la autorización para trabajar sobre cualquier información telemática.

La firma digital permite garantizar tres de las medidas de seguridad de un documento electrónico.

3.4.6. A new Efficient Digital Signature Schema Algorithm based on Block cipher [KUPPUSWAMY, 2012]

La información enviada a través de internet o a través de un medio no controlado o asegurado compromete la integridad y validez de los datos que salen del emisor y llegan al receptor.

Una de las técnicas que permiten asegurar el envío seguro de datos es la firma electrónica, la cual garantiza que el mensaje enviado por el emisor es el mismo que recibe el receptor.

Más aún, si se trata de envío confidencial de datos por parte del gobierno, aplicaciones como comercio electrónico, o pago por internet, deben existir mecanismos seguros que permitan el envío

de datos a sus destinatarios sin sufrir modificaciones en el camino o fuga de datos; por tal razón, la tecnología de PKI ha permitido asegurar el paso de la información de punto a punto.

Una firma digital es un tipo importante de autenticación en un sistema criptográfico de clave pública y es de uso generalizado.

Una firma digital se calcula utilizando un conjunto de reglas y un conjunto de parámetros tales que la identidad del firmante y la integridad de los datos pueden ser verificadas.

Existen otros muchos algoritmos basados en una combinación híbrida de factorización de números primos y algoritmos discretos, pero se ha desarrollado diferentes ataques para descubrir sus vulnerabilidades.

Aqeel Khalique Kuldip y Singh Sandeep Sood propusieron la implementación del algoritmo de Curva Elíptica.

El aporte del autor se verá representado con la implementación de un modelo de algoritmo simétrico que permitirá realizar operaciones criptográficas mucho más rápidas que las internacionalmente adaptadas para firma digital, sin comprometer el grado de seguridad que este pudiera implicar.

El autor demuestra que con este esquema de algoritmos para la firma digital es más rápido el tiempo de ejecución y se tiene la misma seguridad que con los demás algoritmos ya conocidos.

Se puede crear otros algoritmos que mejoren los tiempos de ejecución para realizar la firma digital del mensaje digerido (hash), que sean más rápidos y menos vulnerables a las colisiones.

El proceso que plantean los autores es basarse en el algoritmo de Hill, que recurre al álgebra lineal (matrices) para realizar la firma digital.

El proceso inicia con la generación de una llave aleatoria:

- Asignar el valor n=37.
- Seleccionar una matriz invertible k.
- K debe entregar el resultado k*k*-1 mod 37 = 1.
- Seleccionar cualquier entero y multiplicarlo por k, puede llamarse d.

- Encontrar la inversa del entero y multiplicarlo con la matriz inversa e.

n y e son claves públicas; y d, clave privada.

Si asumimos que el mensaje es “DEAN OMAR”, la representación numérica con la técnica mencionada arriba es 4,5,1,14,15,13,1,18, escogemos la matriz 2x2 , r=2.

Las pruebas realizadas fueron controladas en un equipo Intel Pentium 4, 2.2 Ghz Dual Core, y los algoritmos fueron desarrollados en MATLAB.

Tabla 4: Comparación de rendimiento

Fuente: [KUPPUSWAMY, 2012]

ALGORITHM	NO. OF CHARACTER (MESSAGE)	EXECUTION TIMING
RSA Digital Signature	100	5.6 Seconds
Elgamal Digital Signature	100	6.2 Seconds
Elliptic Curve	100	5.4 Seconds
MD5	100	5.2 Seconds
Proposed DSS	100	5.2 Seconds

Los resultados obtenidos muestran claramente que el algoritmo propuesto, el cual se basa en la iniciativa de algoritmo simétrico de Lester S.Hill (bloque cifrado) con módulo 37 diferente al originalmente planteado (modulo 26), es uno de los algoritmos de firma digital más rápidos y de igual seguridad que los de RSA.

El trabajo plantea los algoritmos de firmas más sofisticados y hace una comparación bastante sencilla de entender.

Existen algoritmos para la firma digital que permiten trabajar de una manera más rápida y manteniendo el nivel de seguridad y garantía.

No se encuentran estandarizados para las aplicaciones recurrentes de firma digital. El más usado es el algoritmo SHA256 de la RSA.

3.4.7. Digital Signature [KAUR, 2012]

Privacidad, Autenticidad, Integridad, No repudio: cuatro factores que garantizar la protección de la información de personas no autorizadas.

Explica la importancia de la utilización de la firma digital a través de técnicas o algoritmos criptográficos para generar el mensaje resumen y para cifrar dicho mensaje a través de la criptografía asimétrica, ya que es más robusta y rápida en comparación con la criptográfica simétrica. Puntualmente, señala que los tiempos de ejecución y verificación al utilizar criptografía simétrica son mayores en comparación con la asimétrica, puesto que se utiliza una única clave privada para firmar y validar el archivo firmado. También se requiere un algoritmo para evaluar la clave simétrica.

Los algoritmos mostrados a continuación son soportados internacionalmente para realizar la firma digital y garantizan la correcta manipulación de los pares de llaves (pública y privada) de la criptografía asimétrica. Estos, a su vez, están incorporados en la FIPS.

La siguiente tabla muestra el tamaño del hash generado por los diferentes algoritmos.

Tabla 5: Algoritmos Hash

Fuente: [KAUR, 2012]

Name of Algorithm	**Type and Characteristics**	Hash Size
Secure Hash Algorithm 1 (SHA1) [8]	FIPS approved; other versions (SHA256, SHA384, SHA512) provide longer outputs	160 bits
Message Digest 5(MD5) [9]	Potential weaknesses is that it can be used as a keyed hash	128bits
RACE Integrity Primitives Evaluation Message Digest 160 (RIPEMD-160) [10]	Developed as part of the EC's Research and Development in Advanced Communications Technologies in Europe (RACE)	160 bit
TIGER Hash [11]	Designed for efficient operation on 64-bit platforms	192 bits

La tabla 6 muestra el tamaño mínimo de las llaves privadas para poder general la firma digital.

Tabla 6: Algoritmos de Firma Digital

Fuente: [KAUR, 2012]

Name of Algorithm	Type and Characteristics	Min. Key Size
Digital Signature Standard (DSS) [5]	FIPS 186-2 digital signature Digital signature based on SHA1 hash, unencumbered (no patents, no licenses)	1024bits
RSA Digital Signature [6]	RSA digital signature (FIPS approved) Previously patented digital signature	1024 bits
Elliptic Curve Digital Signature (ECDSA) [7]	Digital signature based on elliptic curve key technology uses smaller keys than other public key technologies but may be encumbered by various	160 bits

3.4.8. The Application of a Scheme of Digital Signature in Electronic Government [NA, 2008]

La propuesta principal de este trabajo es la utilización de la criptografía simétrica y asimétrica para realizar la firma digital.

Para la criptografía asimétrica, se define una clave privada y una clave pública; y para la criptografía simétrica, una llave secreta. Cabe recalcar que el funcionamiento de este esquema se da solo si previamente se ha compartido la clave pública entre el emisor y el receptor. No aplica para el caso real de una PKI.

Se considera las siguientes llaves:

- Ka1: llave privada del emisor
- Ka2: llave pública del emisor
- Kb1: llave privada del receptor
- Kb2: llave pública del receptor

Se genera el hash del documento original y se realiza inmediatamente la firma digital con sello de tiempo; de igual modo y de manera paralela, se obtiene el mensaje cifrado del documento y se adhiere al documento firmado digitalmente, y la clave pública del receptor se cifra con el algoritmo 3DES. Para los efectos de verificación del documento firmado y con el fin de garantizar la integridad de dicha información, se debe verificar

tanto el hash del documento original embebido como el obtenido luego de descifra la clave secreta.

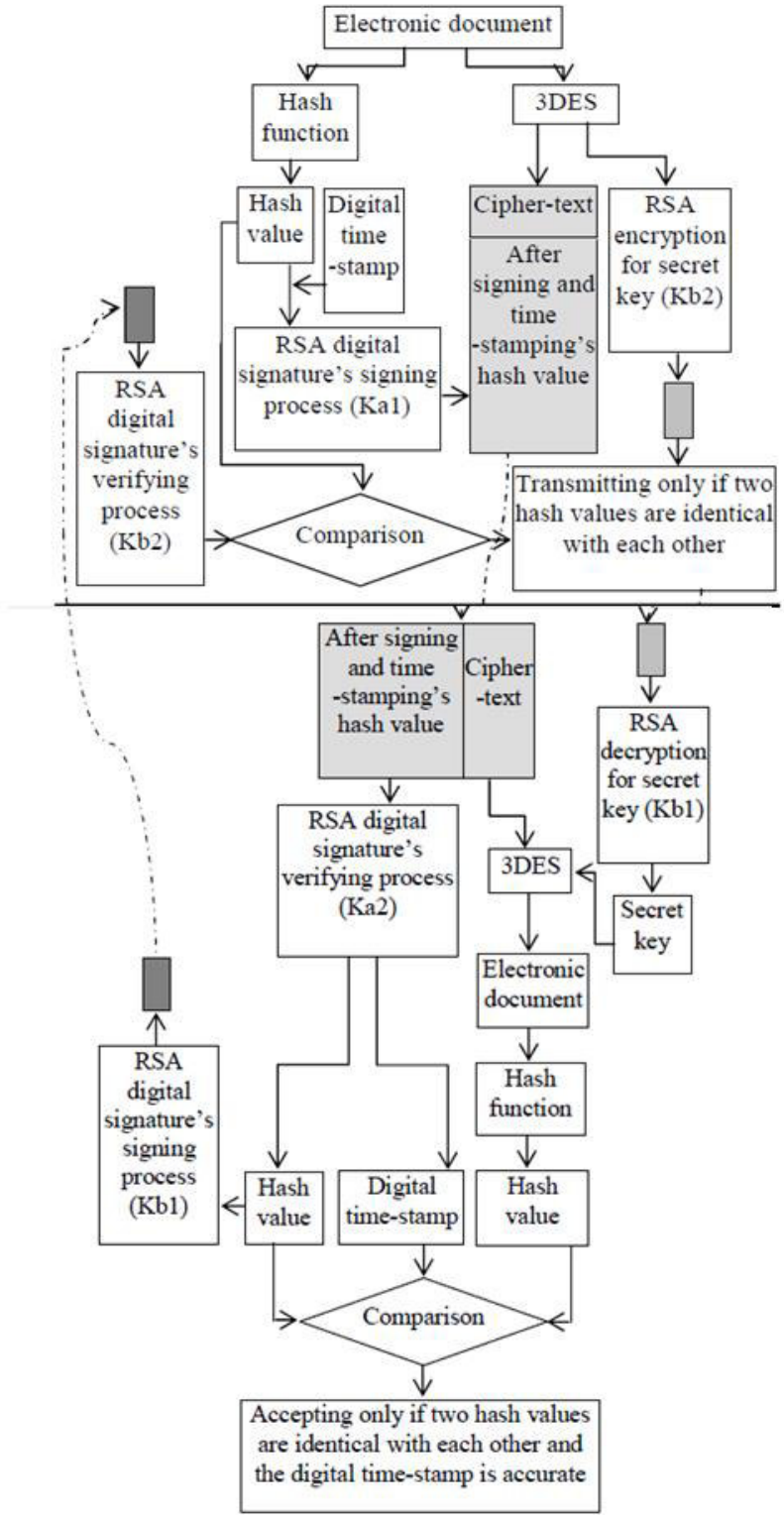


Figura 21: Esquema de Firma Digital

Fuente: [NA, 2008]

Es posible aplicar este esquema en una PKI interna siempre y cuando no se exponga los documentos firmados ante un tercero para su validación.

3.4.9. The Digital Signature Paradox [STAPLETON, 2005]

El autor tiene la finalidad de concientizar acerca del uso de la firma digital, pues si bien esta tecnología nos permite dotar de mecanismos de seguridad a un documento digital, no se tiene control y dominio absoluto sobre los tiempos en los cuales los datos han existido o han sido modificados. Ahora bien, existe un mecanismo llamado sello de tiempo cuya única razón de existir es garantizar de manera certera el momento en el cual los datos o información han existido en un mundo electrónico.

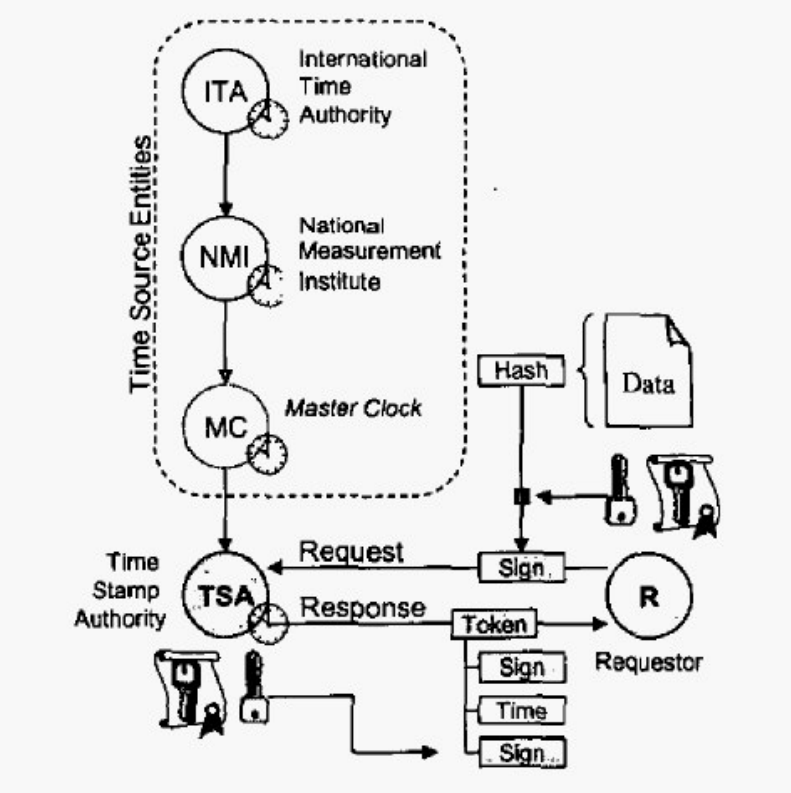


Figura 22: Sello de tiempo de confianza

Fuente: [STAPLETON, 2005]

El autor sugiere una gráfica que explica la confianza heredada que se debe tener para que una Autoridad de Sellado de Tiempo sea considerada de confianza. También lista algunos ejemplos prácticos en los cuales la modificación de los tiempos en los sistemas de información ha impactado en el negocio de diferentes entidades.

3.4.10. Research and implementation of a digital signature scheme based on middleware [FU, 2011]

Se utiliza el algoritmo RSA para la firma digital y el algoritmo MD5 para la generación del hash resumen.

El middleware no es otra cosa que una capa intermedia que permite que los componentes de hardware y software interactúen de manera correcta independientemente de si poseen diferentes interfaces.

En el paper, el autor no menciona concretamente si el certificado que está empleando se encuentra instalado en un sistema operativo Windows, ya que el hecho de utilizar el CSP implica que tanto el certificado como la llave privada asociada a él se encuentran instalados en el repositorio de confianza de Windows.

La figura muestra los diferentes niveles de comunicación desde el hardware hasta una aplicación de alto nivel que ejecuta la firma digital.

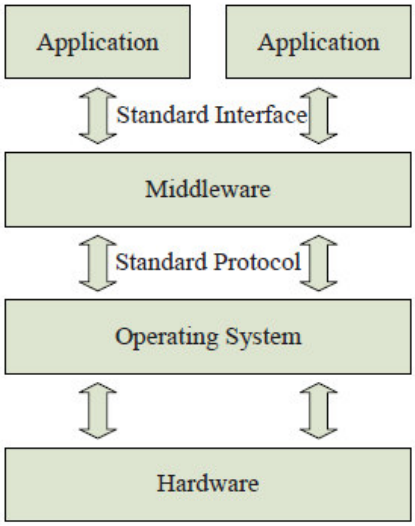


Figura 23: La posición del middleware en un sistema informático

Fuente: [FU, 2011]

Este esquema únicamente funciona dentro de un sistema operativo Windows con ActiveX. Queda fuera del alcance del paper la aplicación para los otros sistemas operativos de escritorio o servidor.

3.4.11. Signing the Document Content is not Enough: a new attack to digital signature [BUCCAFURRI, 2008]

La firma digital representa el único método para entregar el valor probatorio tal cual como la firma manuscrita lo hace en documentos físicos. En la actualidad, el proceso de desmaterialización de los documentos físicos a digitales cobra mayor importancia, y son cada vez más rigurosos los controles para representar en un archivo digital la misma información contenida en un papel.

La realidad es que cuando un documento en físico es firmado, el contenido permanece estático o no es susceptible a variación sin dejar un rastro alguno. Sin embargo, en el mundo digital el contenido es mucho más dinámico y dependiente del origen del documento. Por ejemplo, en un archivo que contenga macros, o código Javascript o inclusive documentos PDF, su tratamiento debe ser muy cuidadoso, ya que los valores pueden variar o ser susceptibles, dependiendo de la fecha del sistema operativo en el cual se visualice dicho archivo. Este incidente podría llevar a riesgos en el futuro si no se controla inicialmente; la manera más trivial es la de forzar al usuario a revisar el documento antes de ser firmado digitalmente, de forma que se garantiza que el usuario estaba consciente que lo que firmaba era lo que en verdad mostraba el documento, de otro modo no existe la firma digital.

Se demuestra un ataque sobre un documento HTML que contiene código que al momento de variar la hora del sistema muestra un valor diferente. Una vez firmado el documento, se cambia la extensión del mismo de picture.bmp.p7m a picture.htm.p7m; y cuando se realiza la validación de la firma digital, se verifica únicamente el contenido del archivo, mas no el nombre del archivo, lo cual presenta una vulnerabilidad.

El autor propone que al momento de generar el hash resumen se considere dentro de la META DATA el nombre del archivo, así como diversos parámetros embebidos en el propio documento.

3.5. CASOS DE ÉXITO

3.5.1. Publicación Certificada – FirmaProfesional (España)

Publifirma es un sistema que permite validar el momento exacto en que una organización publica un documento en su Web, cuánto tiempo permanece publicado y que el documento no ha sufrido ninguna alteración en el periodo de su publicación.

Dicho de otra manera, publifirma aporta a los clientes de Firmaprofesional la evidencia legal de que un documento se publicó en su Web en una fecha y a una hora determinada y durante un período concreto de tiempo y de que el documento no se modificó durante el periodo de publicación.

Ejemplo de uso

- Administraciones Públicas: Publifirma sirve para publicar licitaciones, pliegos, ofertas y otros documentos relacionados con los procesos de contratación.
- Empresas privadas: para la publicación de convocatorias de juntas generales, determinados acuerdos de modificación, acuerdos de reducción o del Derecho estatuario de oposición.

Características principales

- Ahorra tiempo y dinero.
- Aporta evidencia legal de la publicación de documentos en una web.
- Proceso de certificación de publicaciones puede ser manual o automático.

3.5.2. Entidad de Certificación ICERT – EC (Ecuador)

La inicialización de la plataforma de firma electrónica en la función judicial (Plataforma Infraestructura de clave pública), arrancó el 16 de octubre de 2014. El proyecto de firma electrónica pretende reemplazar el uso del papel para todos los trámites judiciales en el país.

Los técnicos del Consejo de la Judicatura de la DNTICS, pertenecientes a la Subdirección Nacional de Seguridad de la Información llevaron a cabo la ceremonia de generación del certificado raíz y subordinado de la entidad de certificación ICERT-EC. Este trámite se realizó en la Corte Nacional de Justicia con la presencia de su presidente, Carlos Ramírez y el titular del Consejo de la Judicatura, Gustavo Jalhk, entre otras autoridades.

Ahora las demandas se podrán presentar a través de la página web de la Judicatura, según explicó el ingeniero Ruperto Amaguai, director encargado de la DNTICS del Consejo de la Judicatura.

Sin embargo, se mantiene la forma tradicional que es de manera escrita en los diferentes tribunales del país.

Secretarios, jueces y abogados podrán registrar sus solicitudes para obtener la firma electrónica en la entidad de Certificación del Consejo de la Judicatura ICERT-EC, el Consejo de la Judicatura almacenará las solicitudes dentro de los servidores instalados en una sala especial de Corte de Justicia donde esta la infraestructura de firma electrónica PKI, que tiene un acceso restringido.

Gustavo Jalkh señaló que el nuevo sistema permitirá que las notificaciones, sentencias y otros documentos judiciales ya no sean emitidos en forma física, esto es un hecho histórico, porque así se avanza hacia el sistema cero papeles, en el que la Judicatura trabaja desde hace algún tiempo.

En la actualidad, los operadores de justicia suscriben a mano decenas de escritos, lo que provoca que los procesos judiciales sean complejos y largos. La nueva herramienta tecnológica dará mayor seguridad y confidencialidad a los documentos, reducirá el uso de millones de hojas de papel y disminuirá el tiempo de los trámites.

“Este primer paso es fundamental para poder utilizar las nuevas tecnologías al servicio de la transparencia, eficiencia, información y justicia”, manifestó

El CJ iniciará un proceso de capacitación a los funcionarios judiciales, jueces y secretarios. El objetivo es que en 2015, con la entrega masiva de la firma electrónica a los operadores de justicia, las notificaciones de carácter informativo que reciben los abogados en su casillero electrónico, tengan plena validez legal.

El sistema cero papeles se complementará con el expediente electrónico, es decir, los abogados en libre ejercicio también contarán, a futuro, con su firma electrónica certificada por el CJ, lo que les permitirá presentar los escritos desde sus despachos, sin necesidad de desplazarse hasta una unidad judicial.

El superintendente de Telecomunicaciones subrogante, Claudio Rosas, sostuvo que el uso de la tecnología y de las telecomunicaciones es fundamental para ejecutar las políticas públicas. Añadió que la firma electrónica garantiza la autoría e integridad de los documentos digitales y fortalece la democratización y universalización tecnológica de la justicia en

Ecuador. Además, “le permitirá al CJ consolidarse como una entidad modelo, preocupada de brindar un mejor servicio”.

3.5.3. Sistema de Intermediación Digital – SUNARP (Perú)

La SUNARP busca evitar la falsificación de instrumentos públicos sobre otorgamiento de poderes, debido a que no se usará papel en el proceso registral sino que se realizará de manera virtual empleando la firma digital.

El otorgamiento de poderes por personas naturales podrá ser inscrito de manera electrónica a partir del 12 de agosto del 2015, a través del SID-Superintendencia Nacional de Registros Públicos (SUNARP), anunció esta institución.

Subrayó que ello garantizará la autenticidad del parte notarial firmado de manera digital por un notario a nivel nacional.

El poder es un documento público autorizado por un notario que permite a una persona nombrar a otra como su representante para que actúe en su nombre en determinados actos jurídicos.

En sus inicios, el Sistema de Intermediación Digital (SID) SUNARP permitía la inscripción registral de las micro y pequeñas empresas (mypes) solo en Lima [SUNARP, 2014].

Mediante la Resolución N° 179-2015-SUNARP/SN el servicio se amplía al ámbito nacional y además se incorpora el otorgamiento de poderes para su inscripción en el Registro de Personas Naturales.

Para ello, es necesario que los notarios cuenten con el certificado digital otorgado por el Registro Nacional de Identificación y Estado Civil (RENIEC) y con una cuenta en el Servicio de Publicidad Registral en Línea (SPRL), además de estar inscritos en el SID-SUNARP.

Para hacer uso de este servicio el ciudadano deberá seleccionar la notaría de su preferencia que se encuentre inscrita al SID-SUNARP, a fin que el notario se encargue de presentar la solicitud de manera virtual a la SUNARP.

El ciudadano a través de este sistema ya no tiene que acercarse a ninguna oficina de la SUNARP.

Solo los notarios podrán enviar el parte notarial de manera virtual a la SUNARP bajo estándares de seguridad. Luego, la SUNARP

notificará el resultado de la solicitud al correo electrónico del ciudadano y del notario.

La lista de notarías afiliadas a este sistema se puede encontrar en https://sid.SUNARP.gob.pe/sid, en la opción “Notarías afiliadas al SID-SUNARP” del Módulo Informativo.

Beneficios del SID-SUNARP

- Impulso de la economía peruana: promueve la constitución de empresas.
- El usuario ya no tendrá que desplazarse hacia una oficina de la SUNARP para realizar sus trámites; si no que ahorrará tiempo y costos de traslado por tratarse de un servicio en línea.
- Se evitará casos de falsificación de documentos, debido a que todo el trámite es virtual, no se usa papel y con firma digital.
- Contribuye a la preservación del medio ambiente ya que el trámite se realiza de manera virtual sin el uso del papel.

3.5.4. Planta de Certificación Digital – RENIEC (Perú)

La Planta de Certificación Digital PKI es un centro de datos altamente especializado que contiene los equipos (hardware), programas computacionales (software) y el personal técnico idóneo, necesarios para cumplir con todos los procesos de certificación digital dentro de un marco regulado por la Infraestructura Oficial de Firma Electrónica - IOFE, cumpliendo, así con los estándares internacionales y procedimientos respectivos.

La Planta de Certificación Digital PKI del RENIEC es la encargada de administrar el ciclo de vida (desde su emisión hasta su cancelación) de los certificados digitales que se otorgarán a las personas naturales y jurídicas en el ámbito nacional.

Se le conoce como Planta de Certificación Digital PKI, por sus siglas en inglés Public Key Infrastructure, cuya traducción al castellano es: Infraestructura de Clave Pública, que es el nombre de la tecnología sobre la cual radica la seguridad del ciclo de vida del certificado digital.

A continuación se brinda un resumen de los componentes de la Planta de Certificación Digital - PKI del RENIEC:

Centro de datos principal:

Es el lugar físico que concentra tanto equipos como personal de la Planta de Certificación Digital, estructurados de tal forma que permiten brindar los servicios de certificación digital con calidad y seguridad.

Consta de 3 áreas:

- Sala de supervisión: Donde se realizan las labores propias de supervisión (supervisión del sistema de control de acceso, sistema de videovigilancia, mesa de ayuda, etc.)
- Sala de máquinas: Es el área que contiene a los equipos críticos de la Planta de Certificación que permiten brindar los servicios de certificación digital de forma continua.
- Sala de operadores: En esta área se realizan las labores de copias de seguridad, monitoreo de servidores, mantenimiento de la Base de Datos, etc.

Centro de datos de contingencia

Es el lugar físico donde se encuentran equipos de respaldo de la Planta de certificación Digital PKI y que funcionan bajo el concepto de alta disponibilidad, además permiten continuar con los servicios de certificación digital en caso ocurra alguna contingencia en el Centro de Datos Principal.

Funcionamiento

La Planta de Certificación Digital PKI, cuenta adicionalmente al Centro de Datos con un Centro de Datos de contingencia, en su afán de brindar un servicio de calidad para los procesos de certificación digital acorde con los más altos estándares internacionales en materia de seguridad de la información así como con la legislación peruana pertinente y de forma específica con la Guía de Acreditación de Entidades de Certificación aprobadas por la Autoridad Administrativa Competente - AAC que indica en el anexo 1, sección 2: "...disponibilidad mínima de 99% anual, con un tiempo programado de inactividad máximo de 0.5% anual".

CAPÍTULO IV: APORTE TEÓRICO

Sobre la base de lo desarrollado en los capítulos del Marco Teórico y el Estado del Arte, se ha logrado explicar el problema de forma clara y precisa; luego de ello, se procederá con la solución al problema principal.

En este capítulo se detallará las herramientas tecnológicas seleccionadas que ayudarán a la implementación de la solución de firma digital web para la Municipalidad de Miraflores a través de la tecnología PKI y la invocación por protocolos.

4.1. REALIDAD TECNOLÓGICA DE LA MUNICIPALIDAD DE MIRAFLORES

Antes de proceder con la selección de las herramientas tecnológicas que permitirán el desarrollo de la solución, es vital conocer la realidad tecnológica de la Municipalidad de Miraflores, con el fin de encontrar consistencia en la implementación del modelo de firma digital web y la aplicación de workflow.

4.1.1. Lado Cliente

Las estaciones de trabajo de los usuarios se encuentran dentro de la misma red institucional de la Municipalidad de Miraflores. Son computadores del tipo desktop o escritorio.

- Sistema Operativo: Microsoft Windows 7 (x86)
- Navegador web: Microsoft Internet Explorer v11.0

4.1.2. Lado Aplicación

La naturaleza de la aplicación y de las herramientas de desarrollo dentro de la Municipalidad de Miraflores es la siguiente:

- IDE: Eclipse Kepler
- Lenguaje de Programación: Java web
- JDK: JDK 7
- Sistema Operativo: Microsoft Windows 7 (x86)

4.1.3. Lado Servidor

Las características del servidor de la Municipalidad de Miraflores son las siguientes:

- Software de Virtualización: VMware ESXi 5.5
- Sistema Operativo: CentOS 6.x (x64)

- Servidor de Aplicaciones: Apache Tomcat 7
- Hardware servidor: Servidor Cisco UCS220 M3
- Procesador : Intel E5-2640 6 Core (12 Threads)
- Memoria RAM: 64 GB
- Almacenamiento: 4TB en NetApp

4.2. SELECCIÓN DE LAS HERRAMIENTAS TECNOLÓGICAS

Una vez conocida a fondo la infraestructura tecnología de la cual dispone la Municipalidad de Miraflores, se procederá a seleccionar las herramientas necesarias para dar solución al problema y lograr satisfacer los objetivos principales y secundarios.

4.2.1. Selección del lenguaje de programación

El lenguaje de programación web es JAVA, dado que la aplicación de workflow de la Municipalidad de Miraflores está desarrollada íntegramente bajo este lenguaje de programación.

4.2.2. Selección de algoritmos de cifrado Hash

Según la investigación realizada y los documentos normativos para el estado peruano que se explican con mayor detalle en el Estado de Arte, se procederá a realizar una comparación de los diferentes algoritmos de cifrado para la realización de la firma digital y se acoja a las disposiciones de la IOFE.

En la siguiente tabla se establecen los criterios de evaluación considerados para la selección del algoritmo hash más adecuado.

Tabla 7: Criterios de Evaluación de los algoritmos de Hash

Fuente: [Elaboración propia]

		VALOR	DESCRIPCION	Puntaje
CRITERIOS	Complejidad de Hardware	Media	Nivel de seguridad de utilización del algoritmo en un hardware criptográfico.	1
		Media-alta		2
		Alta		3
	Estado Actual	Colisionado	Si el algoritmo se encuentra a la fecha vulnerable a un ataque de fuerza bruta o colisión	0
		No colisionado		1

	Tamaño de Hash	128bits	Tamaño final de un mensaje hash de resumen	1
		160bits		2
		192bits		3
	Operaciones Lógicas	AND,OR,NOT,Rotating shifts	Operaciones lógicas soportadas con los dispositivos criptográficos.	1
		AND,OR,NOT,Rotating shifts,XOR		2

Tabla 8: Evaluación de Algoritmos Hash según criterios

Fuente: [Elaboración Propia]

Criterios		Algoritmos HASH		
		SHA1	SHA2	MD5
C1	Complejidad de Hardware	2	3	1
C2	Estado Actual	0	1	0
C3	Tamaño de Hash	2	3	1
C4	Operaciones Lógicas	2	2	1
TOTAL		6	9	3

Entre los algoritmos consultados y analizados en la Tabla 8, se recomienda el uso del SHA2 por su robustez y velocidad de procesamiento en comparación con los demás algoritmos. [NOROOZI, 2013], [NIST, 2011].

4.2.3. Selección del algoritmo de firma digital

Según la investigación realizada y los documentos normativos para el estado peruano que se explican con mayor detalle en el Estado de Arte, se procederá a realizar una comparación de los diferentes algoritmos de cifrado para la realización de la firma digital y se acoja a las disposiciones de la IOFE.

En la siguiente tabla se establecen los criterios de evaluación considerados para la selección del algoritmo de firma digital más adecuado.

Tabla 9: Criterios de Evaluación de los algoritmos de Firma Digital

Fuente: [Elaboración propia]

		VALOR	DESCRIPCION	Puntaje
CRITERIOS	Tiempo de Ejecución	<= 5.2 segundos	El tiempo de ejecución del algoritmo	3
		<5,2 ; 6 > segundos		2
		>= 6 segundos		1
	Numero de caracteres del	<100	El número de caracteres que	3
		=100		2

	mensaje	>100	soporta el algoritmo	1
	Certificado por FIPS	SI	El algoritmos ha pasado satisfactoriamente la auditoria de FIPS que garantiza que es un algoritmo seguro	1
		NO		0
	Tamaño de clave mínimo	1024bits	El mínimo de clave para realizar la firma digital.	1
		160bits		2

Tabla 10: Evaluación de Algoritmos de Firma Digital según criterios

Fuente: [Elaboración Propia]

Criterios		Algoritmos de Firma Digital		
		RSA DSA	DSS	ECDSA
C1	Tiempo de Ejecución	2	1	2
C2	Numero de caracteres del mensaje	2	2	2
C3	Certificado por FIPS	1	1	0
C4	Tamaño de clave mínimo	1	1	2
TOTAL		6	4	6

Según la evidencia de la evaluación reflejada en la Tabla 10 el algoritmo de firma digital seleccionado es RSA DSA. Existen otros tipos de algoritmos de firma digital consultados en el estado del arte, pero no serán empleado, ya que los estándares de certificación FIPS 140-2 y Common Criteria (Ver Anexos) no los encuentran reconocidos como seguros dentro del chip criptográfico. [NIST, 2011].

4.2.4. Selección de contenedor criptográfico

De entre los dispositivos criptográficos explicados en el Estado del Arte y con la aclaración que la Municipalidad de Miraflores requiere un contenedor criptográfico tipo Token, se hizo un estudio en el mercado de algunos tokens comercializados en el Perú. Se procede a hacer un Benchmarking de estos a fin de seleccionar la mejor solución para este caso.

En la siguiente tabla se establecen los criterios de evaluación considerados para la selección del token criptográfico a emplear.

Tabla 11: Criterios de Evaluación de los Tokens criptográficos

Fuente: [Elaboración propia]

		VALOR	DESCRIPCION	Puntaje
CRITERIOS	Certificación FIPS / Common Criteia	Cumple	Certificación internacional que avala que el token es un dispositivo seguro que permite realizar operaciones criptográficas seguras.	1
		No cumple		0
	MiniDriver	Soportado	Es el driver para ser instalado en cualquier versión de Windows para escritorio.	1
		No soportado		0
	Librería PKCS#11	Si	Si el proveedor proporciona dicha librería propietaria para poder funcionar	1
		NO		0
	TokenD	Soportado	Permite operar con el sistema operativo MAC OSX	1
		No soportado		0
	Reemplazo del chip cuando se bloquea	SI	Permite reemplazar el chip criptográfico sin necesidad de adquirir un nuevo token	1
		NO		0
	Software de Firma portable y acreditado ante INDECOPI	SI	El software debe estar contenido dentro del mismo token y es independiente de cualquier otra tecnología	1
		NO		0
	Software de Validación portable y acreditado ante INDECOPI	SI	El software debe estar contenido dentro del mismo token y es independiente de cualquier otra tecnología	1
		NO		0

Tabla 12: Evaluación de Tokens criptográficos según criterios

Fuente: [Elaboración Propia]

Criterios		Algoritmos de Firma Digital		
		cryptoKEY	iAM	eToken 7300
C1	Certificación FIPS / Common Criteia	1	1	1
C2	MiniDriver	1	1	1
C3	Librería PKCS#11	1	1	1
C4	TokenD	1	1	0
C5	Reemplazo del chip cuando se bloquea	1	1	0
C6	Software de Firma portable y acreditado ante INDECOPI	0	1	0
C7	Software de Validación portable y acreditado ante INDECOPI	0	1	0
TOTAL		5	7	3

Después del análisis presentado en la Tabla 12, el token seleccionado en esta oportunidad es el token iAM, ya que, además de ser un contenedor criptográfico, posee un software de firma portable que se ejecuta en su memoria flash interna y es totalmente independiente de la aplicación de workflow de la Municipalidad, lo cual otorgará la facilidad de poder realizar firmas digitales fuera de la intranet.

4.3. ADAPTACIÓN DE HERRAMIENTAS TECNOLÓGICAS

4.3.1. Definiendo la Arquitectura de firma digital web

Se presenta la interacción de los componentes responsables para la realización de la firma digital dentro de la infraestructura tecnológica de la Municipalidad de Miraflores.

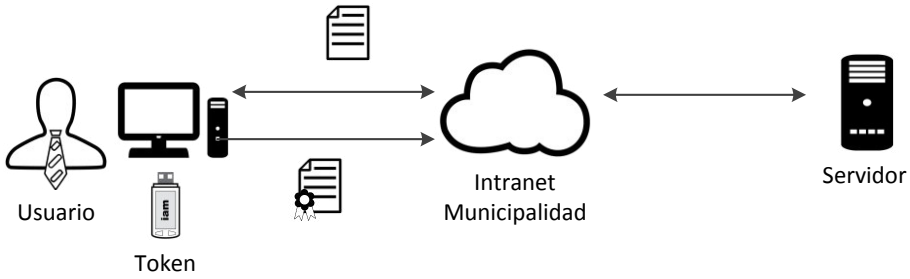


Figura 24: Modelo de Firma Digital

Fuente: [Elaboración propia][7]

4.3.2. Diagrama de Secuencias

Este diagrama muestra la secuencia ordenada de cada componente al momento de hacer la firma digital.

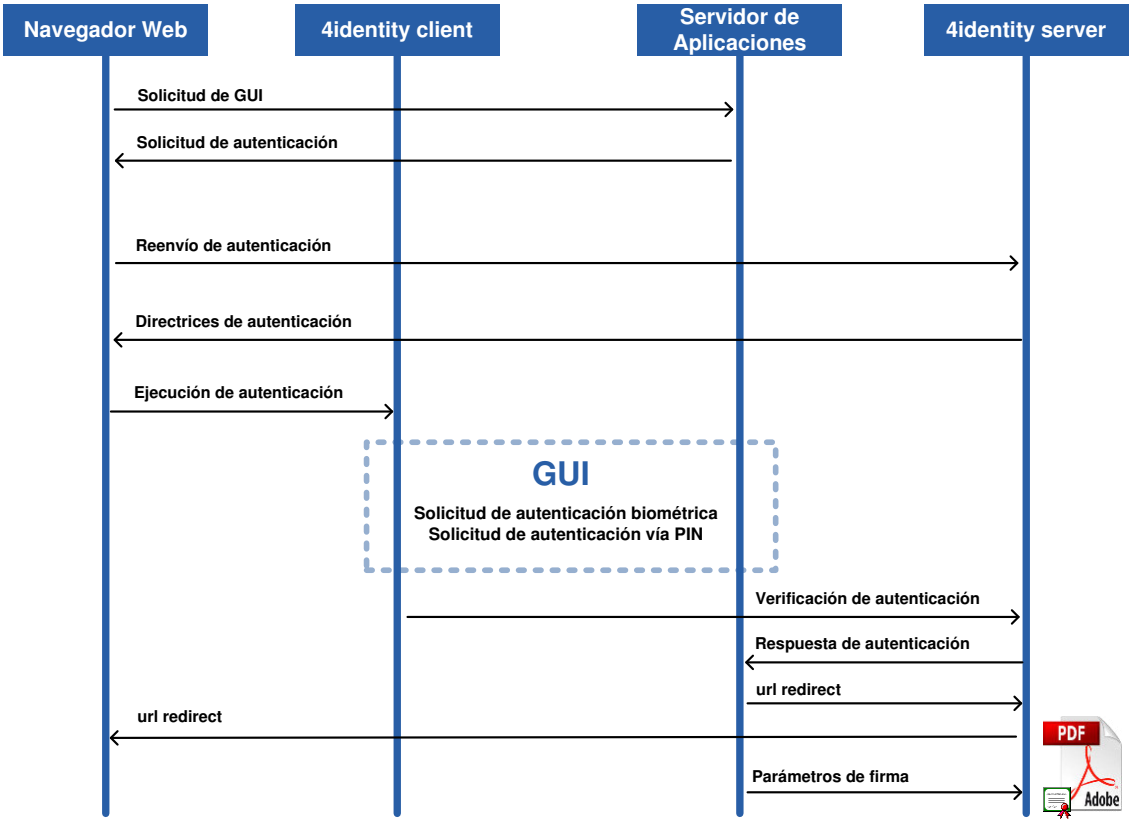


Figura 25: Flujo de firma digital

Fuente: [BIT4ID, 2015]

4.4. BENCHMARKING

Existen actualmente diversos motores criptográficos en el mercado que permiten realizar firma digital de archivos electrónicos.

[7] Los iconos fueron proporcionados por BIT4ID.

4.1.1. Xolido

(http://www.xolido.com/)

Es un software cliente que permite realizar firmas digitales a cualquier tipo de archivo. Soporta los siguientes estándares internacionales:

- CAdES-BES y CAdES-EPES.
- XAdES-BES y XAdES-EPES.
- PAdES-BES y PAdES-EPES. (solo soporta la firma digital y no sello de tiempo)

Soporta la firma en lotes de archivos indicándolos de uno a uno y permite la personalización de la marca gráficas en los archivos PDF.

Adicionalmente, soporta el sellado de tiempo; no obstante, no se puede realizar la firma y sello de tiempo a la vez.

Muestra muchas opciones para personalizar la firma, lo que puede resultar bueno o malo para usuarios inexpertos.

4.1.2. Refirma

(http://portales.RENIEC.gob.pe/web/dni/aplicaciones)

Es un motor de firmas digitales acreditado dentro del marco de la Infraestructura Oficial de Firmas Electrónicas (IOFE) por INDECOPI.

Es una aplicación cliente desarrollada íntegramente en el lenguaje de programación de Java que solo trabaja en sistemas operativos de la familia de Windows. Adicionalmente requiere una instalación del Java Runtime Environment (JRE) 6 o superior de 32 bits.

- Permite firmar digitalmente documentos en formato .pdf.
- Firma solo un archivo PDF a la vez y no un lote de archivos.
- Solo es posible realizar la firma digital con el DNIe de la República del Perú.

El refirma de RENIEC es un software del tipo cliente que realiza la firma digital de únicamente documentos PDF en el formato PAdES. Soporta la firma gráfica, pero no el Long Term Value (firma longeva), para permitir la validación en un momento posterior en el tiempo, sin conexión a Internet.

4.1.3. 4identity

Es un framework que permite la integración de la firma digital independientemente del lenguaje de programación web que se utilice.

Soporta todos los estándares estudiados de firma digital, así como también la firma longeva y sellada de tiempo.

Es un motor de firmas digitales acreditado en el marco de la Infraestructura Oficial de Firmas Electrónicas (IOFE) por INDECOPI.

Posee una aplicación nativa desarrollada en Python y una parte servidor que autoriza cada petición de firma proveniente de un cliente web con los parámetros mandatorios. Se descarga un script que activa esta aplicación nativa y se procede con la firma digital.

No es un modelo cliente servidor, ya que, por motivos de seguridad, la clave privada del certificado digital asociado al portador de un token o smart card no se puede exportar en la operación.

El presente Benchmarking cosiste en evaluar estos motores de firma explicados anteriormente según los criterios que se explicaran a continuación:

C1- Independencia de tecnología JAVA: Si la solución o tecnología no depende de ningún componente, Java Virtual Machine, applets o librería Java en general. [NIST, 2014]

C2 - Independencia de ActiveX: La independencia de la tecnología Microsoft y sobre todo la independencia del componente ActiveX permitirá una mejor accesibilidad [HUN, 2012].

C3 - Soporte de TSA externa: La necesidad de incrustar un sellado de tiempo al momento de la firma digital permitirá asegurar que los datos existieron en una determinada fecha y hora.

C4 - Acreditación ante INDECOPI: Deben haber superado satisfactoriamente las guías de acreditación de software de firma digital en el marco de la IOFE [INDECOPI, 2008].

C5 - Firma en lotes: La posibilidad de realizar el mismo tipo de firma a más de una documento por vez permite un mayor

practicidad al usuario ya que bastará con colocar una sola vez el PIN para que se pueda realizar la firma digital.

C6 - Firma en formato PAdES: Este tipo de formato permite realizar la firma digital en tipos de archivos tipo PDF o especiales como PDF/A. [ETSI, 2009].

C7 - Firma gráfica: Según el estándar PAdES, es posible añadir una imagen o representación gráfica asociada a la firma digital para cualquier tipo de documento con extensión PDF [ETSI, 2009].

C8 - Firma en formato CAdES: Este tipo de formato permite la firma digital de cualquier tipo de documento electrónico, no exclusivamente del tipo PDF [ETSI, 2012].

C9 - Firma en formato XAdES: Este tipo de formato permite la firma de documentos con extensión .xml o en general de cualquier archivo basado en una estructura de datos [ETSI, 2010].

C10 - Multiplataforma: Este criterio hace mención de que el software pueda ser ejecutado y soportado en un sistema operativo de escritorio.

C11 - Permite utilizar otros middlewares: Debe permitir la incorporación de otros midllewares propietarios sin necesidad de hacer uso del CSP de Windows.

C12 - Es integrable en web: Debe permitir la integración con cualquier navegador web.

Los puntajes establecidos para cada uno de los criterios descritos anteriormente corresponderán la siguiente escala:

Si cumple satisfactoriamente se asigna el valor de: 2

Si cumple mínimamente se asigna el valor de: 1

No cumple le asignamos el valor de: 0

Tabla 13: Benchmarking de motores criptográficos

Fuente: [Elaboración propia]

CRITERIOS	Xolido	Refirma	4identity
C1	1	0	2
C2	2	1	2
C3	2	0	2
C3	2	0	2
C5	2	1	2
C6	2	1	2
C7	2	1	2
C8	2	0	2
C9	2	0	2
C10	1	1	2
C11	2	1	1
C12	0	0	2
TOTAL	20	6	23

Según al análisis que se observa en la Tabla 13 se concluye que la mejor opción para el presente trabajo es la solución 4identity ya que permite una mayor versatilidad en comparación de las demás soluciones consideradas.

CAPÍTULO V: APORTE PRÁCTICO

En este capítulo se explica sobre qué tecnologías se pretende desplegar la implementación del presente modelo de firma digital web según el capítulo IV.

También se explica las configuraciones preliminares del lado del cliente y del servidor necesarias para la posterior implementación.

5.1. LADO CLIENTE

Para poder realizar la firma digital con las herramientas seleccionadas, se debe realizar las siguientes tareas:

5.1.1. Instalación de 4identityclient.exe

La siguiente instalación corresponde a un cliente con plataforma basada en Windows.

La instalación de este cliente nativo permitirá la realización de las siguientes funciones:

- Descarga del archivo desde el servidor al cliente.
- Pre-visualización del archivo PDF.
- Listar y seleccionar el certificado digital a utilizar.
- Firmar digitalmente el archivo.

Basta con hacer doble clic en el archivo 4identityclient.exe para que se inicialice el asistente de instalación de Windows como se muestra en la figura.

Figura 26: Asistente de instalación de Windows

Fuente: [BIT4ID, 2015]

Al finalizar la instalación del 4identyclient.exe aparecerá la siguiente ventana.

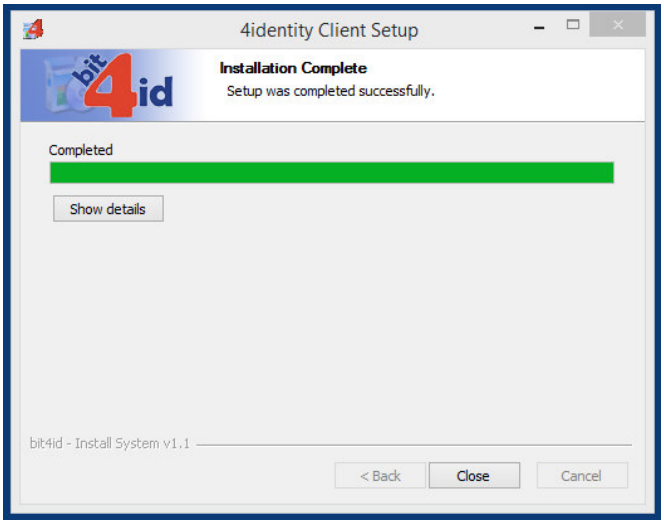


Figura 27: Instalación completada

Fuente: [BIT4ID, 2015]

5.1.2. Instalación del Middleware

Los dispositivos criptográficos a emplear son los tokens criptográficos iAM de BIT4ID. Para que se puedan comunicar con la aplicación web de firma digital, es imprescindible la instalación del middleware del chip para poder realizar operaciones criptográficas.

Una vez finalizada la instalación, se recomienda reiniciar el equipo para que los cambios se efectúen.

5.2. LADO SERVIDOR

La presente configuración corresponde a una plataforma basada en Linux.

La instalación del servidor permitirá las siguientes funciones:

- Establecer canal seguro con el cliente.
- Descarga del script al cliente para que se ejecute la aplicación nativa 4identityclient.exe.

5.2.1. Instalación del servidor

Se debe crear un folder en donde se almacene la configuración.

Por ejemplo: **mkdir /opt/bit4id**

Copiar los archivos **connector.tar.gz** en la ruta /**opt**/

Ejecutar el siguiente comando para descomprimir los archivos:

tar -xvzf connector.tar.gz -C /opt/bit4id

5.2.2. Creación de servicio

Se crea un nombre de servicio asociado a través del siguiente comando:

/opt/bit4id/connector/bin

Para establecer el nuevo servicio, se debe ejecutar el siguiente comando:

./license utils add --name <<FRIENDLY_NAME>> --port <<PORT>> --license <<LICENSE_FILE>>

En donde:

<<FRIENDLY_NAME>>: Es el nombre amigable que identificará el servicio de firma.

<<PORT>>: Es el Puerto de servicio.

<<LICENSE_FILE>>: Es la ruta donde se encuentra el archivo de licencia.

CAPÍTULO VI: IMPLEMENTACIÓN

En este capítulo se describe las tecnologías que soportarán la solución de firma digital que está compuesta de un lado cliente y un lado servidor.

6.1. LADO CLIENTE

Se debe instalar el componente 4identityclient.exe, el cual se encargará de realizar la firma digital. La instalación se resume en un simple asistente de instalación estándar.

Luego se desarrolla un cliente web en lenguaje Java para que pueda enviar los parámetros de firma digital al lado servidor y se establezca un canal de comunicación cliente/servidor.

index.html

```
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>EJEMPLO DE FIRMA DIGITAL</title>
</head>

<body>
<div>
    <form class="bit4id-sign" action="identity/Signing" method="post" >

        <p></p>
         <div class="bit4id-signReq" style="display: none;">

        <div class="bit4id-
document">http://localhost:8080/identity/carpeta/miraflores.pdf</div>

        <div class="bit4id-documentName">reporte.pdf</div>
        <div class="bit4id-documentID">aqui_nom_doc.pdf</div>
        <div class="bit4id-signatureType">PAdES</div>
        <div class="bit4id-signingAlgorithm">RSASHA256</div>
        <div class="bit4id-certInfo">CN</div>

      </div>
      <div>
              <fieldset>
        <div><h3>Pagina WEB de firma digital</h3></div>
        <div><p><strong>Se procedera a firmar digitalmente el archivo
reporte.pdf, esta seguro de continuar?</strong></p></div>
        <div id="bit4id-status"></div>
```

```
          <div><input type="submit"  value="Sign Document"
name="cmd"/></div>

        </fieldset>
      </div>
    </form>
     <script src="http://as-demo.bit4id.org/smartengine/bit4id-
sign.min.js"></script>
      </div>
</body>
</html>
```

Esta página contiene el elemento form con una clase personalizada llamada: *bit4id-sig*, la acción recae contra el servlet **Signing.java** y en método **POST**.

```
<form class="bit4id-sign" action="identity/Signing" method="post" >
```

Este form es llenado con la siguiente información:

- La ruta del archivo: http://localhost:8080/identity/carpeta/miraflores.pdf
- El nombre del archivo: reporte.pdf
- El identificador del archivo: aqui_nom_doc.pdf
- El tipo de firma a realizar: PAdES
- El algoritmo de firma: RSASHA256
- El nombre común: CN
- Información del canal de conexión entre el cliente y el servidor, para fines de bebug:
- El botón submit para enviar el post, el nombre necesario para el cmd y disabled: <input type="submit" value="Sign Document" name="cmd"/>
- El recurso script que se encuentra en el servidor desplegado:<script src="http://fe.example.com:8082/smartengine/bit4id-sign.min.js"></script>

Se despliega la aplicación web desarrollado en Java sobre el servidor web Apache Tomcat, y se espera la comunicación con el lado servidor.

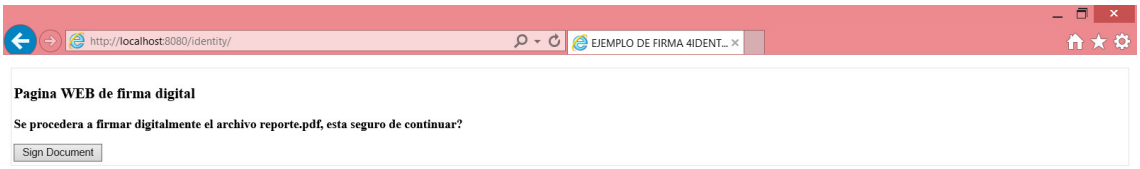


Figura 28: Inicio de la aplicación

Fuente: [Elaboración propia]

El navegador web reconoce una petición externa, hecha desde un servidor, para activar una aplicación nativa, en este caso el 4identyclient.exe, el cual pregunta al usuario si desea permitir o no la ejecución de este programa.

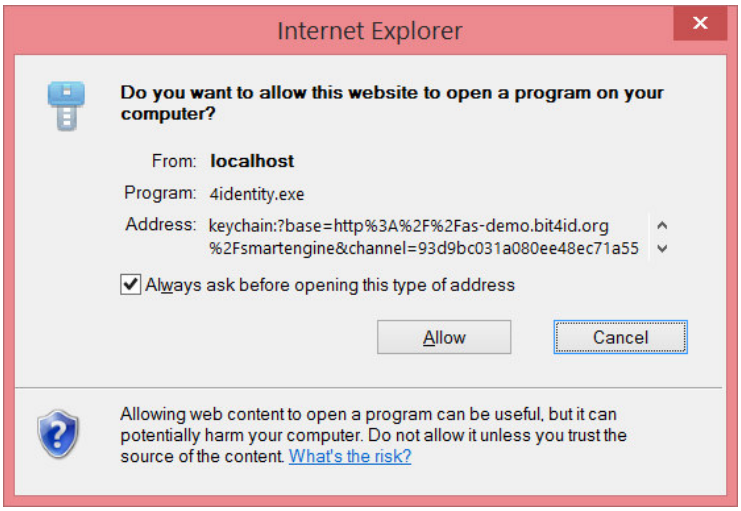


Figura 29: Solicitud de invocación por protocolos[8]

Fuente: [Elaboración propia]

Una vez que el usuario permite la ejecución de la aplicación nativa que reside en su computadora, se activa el botón “Sign Document” dentro del portal web cliente.

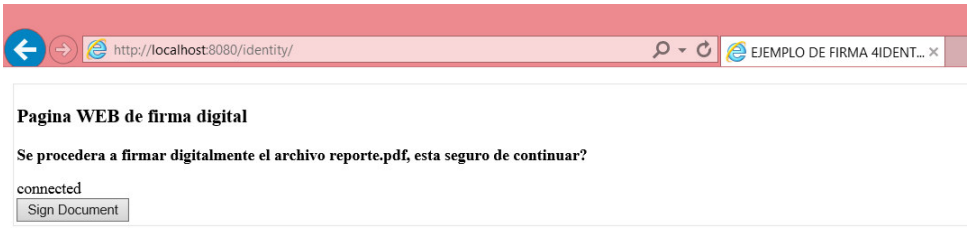


Figura 30: Activación del botón de Sign Document

Fuente: [Elaboración propia]

[8] Autorización de peticiones externas para activar programas nativos a través de Internet Explorer.

El archivo a firmar es descargado localmente (en la computadora del usuario) y de manera transparente para el usuario. Luego se listan todos los certificados que reconoce el CSP de Windows como se muestra en la figura 31.

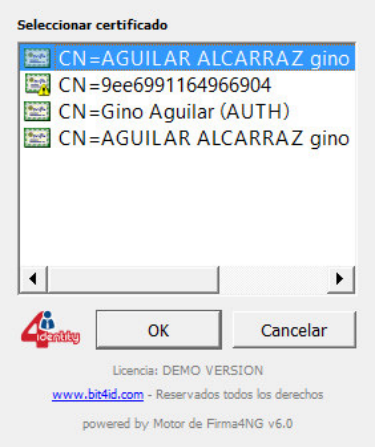


Figura 31: Lectura de certificados digitales[9]

Fuente: [Elaboración propia]

Como siguiente paso, y tras la selección y aprobación del certificado a utilizar, la aplicación nativa ejecuta una pre visualización del archivo PDF antes de llevar a cabo la firma digital.

[9] La lectura referente a los certificados digitales a través del 4identitycliente.exe.

Figura 32: Pre visualización de documento PDF[10]

Fuente: [Elaboración propia]

Observación: Si el archivo que se pretende firmar no es un archivo en formato PDF, entonces se despliega la siguiente ventana. Ver figura 33. Si el usuario confía en el documento a firmar, basta con que haga clic en el botón “firmar”; pero si se requiere visualizar el archivo antes de la firma, el usuario debe hacer clic en el botón “Abrir documento”, el cual consultará en el Registro de Windows cuál es la aplicación por defecto asociada para abrir ese tipo de archivos.

[10] Previsualizador nativo de archivos PDF incorporado en el 4identitycliente.exe.

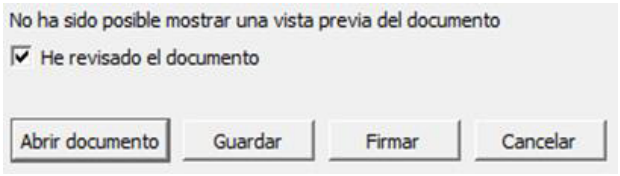


Figura 33: Ventana de verificación de firma del archivo[11]
Fuente: [Elaboración propia]

Después de aceptar cerciorarse del documento a firmar yd el certificado digital a utilizar, el propio CSP de Windows solicita el ingreso del PIN para autorizar el proceso criptográfico de firma digital.

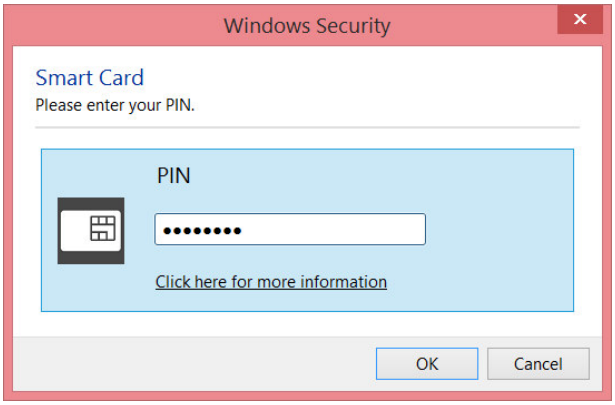


Figura 34: Solicitud de ingreso del PIN[12]

Fuente: [Elaboración propia]

El 4identityclient.exe llama de forma inmediata y transparente a success.jsp, que es una página en el lado del cliente que permite la generación de un link que apunta al archivo firmado para que este pueda ser descargado una vez se haya procedido con la firma digital.

success.jsp

```
<%@ page language="java" contentType="text/html; charset=ISO-8859-1"
    pageEncoding="ISO-8859-1"%>
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
```

[11] Imagen generada por el 4identityclient.exe
[12] Ventana emergencia gracias al CSP de Windows, para realizar operaciones criptográficas.

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-
8859-1">
<title>Signature Process</title>
</head>
<body>
<%

if (request.getParameter( "link" ) != null) {
        String link = request.getParameter("link");
        out.println("<a href=" + link.toString() + ">ARCHIVO
FIRMADO</a>") ;

}

if (request.getParameter( "outprint" ) != null) {
        String outprint = request.getParameter("outprint");
        out.println("REQUEST PRINT:" + outprint.toString());
}

%>

</body>
</html>
```

Una vez descargado el archivo PDF firmado, este puede ser abierto con cualquier visualizador PDF convencional. En este caso, se está utilizando el programa Adobe Reader 11.0.13, que soporta la visualización de un panel de firma digitales.

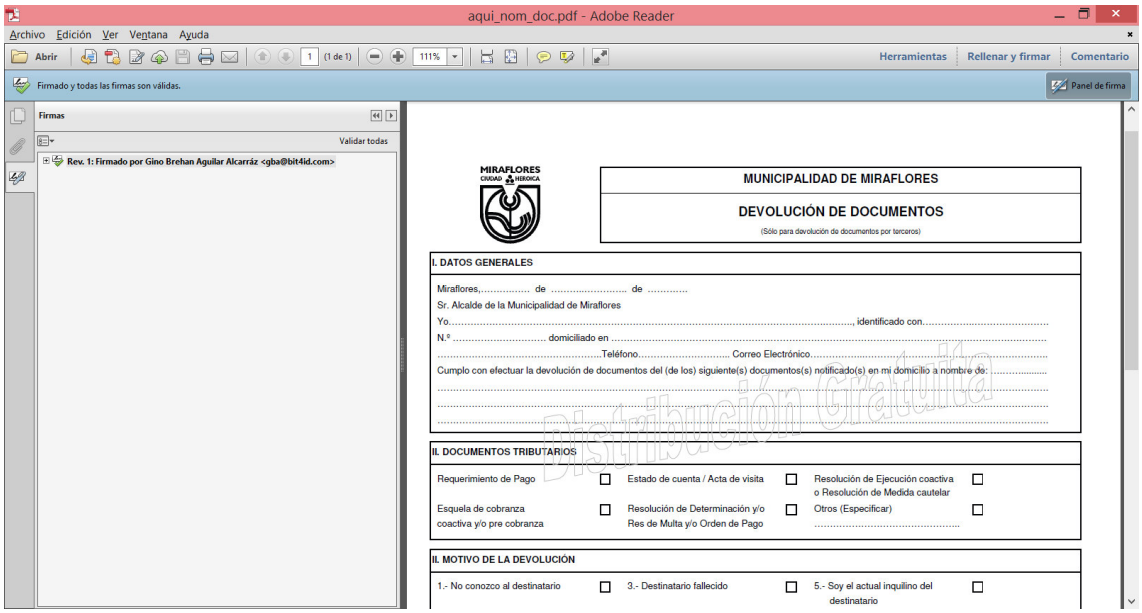


Figura 35: Visualización de documento PDF firmado digitalmente

Fuente: [Elaboración propia]

6.2. LADO SERVIDOR

Dentro del lado del servidor y luego de haberse ejecutado la firma digital en el cliente, mediante un servicio POST se recoge los bytes firmados del archivo PDF original y se los reconstruye en PDF firmado en el lado del servidor, para su posterior descarga con el **success.jsp.**

Signing.java

```
package com.bit4id.identity;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.File;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.io.PrintWriter;
import javax.servlet.ServletContext;
import javax.servlet.ServletException;
import javax.servlet.annotation.MultipartConfig;
import javax.servlet.annotation.WebServlet;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import javax.servlet.http.Part;
```

```
@WebServlet("/Signing")
@MultipartConfig(fileSizeThreshold=1024*1024*10,maxFileSize=1024*
1024*15,maxRequestSize=1024*1024*30)
public class Signing extends HttpServlet {
	private static final long serialVersionUID = 1L;


	public Signing() {
	super();

   }

	@Override
	protected void doGet(HttpServletRequest request,
HttpServletResponse response) throws ServletException, IOException
{
		PrintWriter out = response.getWriter();
		out.println("SIGNATURE MANAGEMENT SERVLET");


		ServletContext servletContext = getServletContext();
		String contentdir =
servletContext.getRealPath(File.separator);
		String pathServlet = request.getServletPath();
		String fullPathServlet = request.getRequestURL().toString();
		int resInt = fullPathServlet.length() - pathServlet.length();

		String result = fullPathServlet.substring(0, resInt + 1);

		out.println("Context path: " + contentdir);
		out.println("Full Servlet path: " + fullPathServlet);
		out.println("Servlet path: " + pathServlet);
		out.println("Server path: " + result);


		out.close();
	}

	@Override
	protected void do|(HttpServletRequest request,
HttpServletResponse response) throws ServletException, IOException
{


		ServletContext servletContext = getServletContext();
		String contentdir =
servletContext.getRealPath(File.separator) + "signed";

		String pathServlet = request.getServletPath();
		String fullPathServlet = request.getRequestURL().toString();
```

```
                int resInt = fullPathServlet.length() - pathServlet.length();


                String signstore = fullPathServlet.substring(0, resInt + 1) +
"signed";

                String fileName = null;
                String tempFileDestination = null;
                  for (Part part : request.getParts()) {
                        if (part.getName().equals("documentID")) {
                                InputStream inputStream =
part.getInputStream();

                                InputStreamReader inputStreamReader =
new InputStreamReader(inputStream);
                                BufferedReader bufferedReader = new
BufferedReader(inputStreamReader);

                                        fileName = bufferedReader.readLine();
                        } else if (part.getName().equals("attach")) {
                     tempFileDestination = contentdir + File.separator +
"temp.pdf";
                                        part.write(tempFileDestination);
                        }
                        }


                new File(tempFileDestination).renameTo(new
File(contentdir + File.separator, fileName));
                response.sendRedirect("success.jsp?link=" + signstore +
"/" + fileName);


        }

}
```

CAPÍTULO VII: CONCLUSIONES Y TRABAJOS FUTUROS

7.1. CONCLUSIONES

Luego de haber revisado la bibliografía, se presenta las conclusiones obtenidas por el autor. Se afirma lo siguiente:

- La implementación de un componente de firma digital web dentro de la municipalidad ha sido posible considerando la tecnología del 4identity (ver Tabla 3.6), algoritmo de firma digital RSA (ver Tabla 4.4), algoritmo de Hash SHA2 (ver Tabla 4.2) y el contenedor criptográfico tipo token iAM (ver Tabla 4.6).
- Se ha podido evitar cualquier tipo de independencia de tecnología Java, ActiveX, navegador web, que dificulta la integración y la accesibilidad a las aplicaciones web, y así se cumple el objetivo secundario #1. [HUN, 2012]
- Se ha podido realizar la integración en cualquier navegador haciendo uso de la invocación por protocolos de una aplicación nativa y el uso de un token criptográfico cumpliendo el objetivo secundario #2 [RUNDGREN, 2015] y #5 [CONGRESO DE LA REPÚBLICA DEL PERÚ, 2001] simultáneamente.
- Los gerentes y subgerentes pueden realizar la firma digital con pleno valor legal haciendo uso de este software acreditado ante INDECOPI [INDECOPI, 2008] y el dispositivo criptográfico tipo token iAM, cumpliendo así el objetivo secundario #3 y #4 simultáneamente.
- Con esta nuevo workflow con firma digital web ya no será necesario demandas todas las hojas que la Municipalidad utiliza para imprimir su información y realizar la firma manuscrita, se cumple así el objetivo secundario #6.
- Los dispositivos criptográficos proporcionan mecanismos de seguridad a nivel hardware y software para el uso adecuado de los certificados digitales que residen en él, y deben cumplir con las certificaciones FIPS 140-2 o Common Criteria. Estos no son excluyentes entre sí y dependen de la región en donde se utilicen. [NIST, 2015]
- La seguridad de la firma digital se concentra en el hash resumen de cada documento a firmar. Puesto que se trata de una operación unidireccional, provee la total garantía de que no existe otro documento que pueda generar el mismo hash a través del mismo algoritmo Hash. [PARAG, 2014].
- La firma digital provee la integridad, autenticidad y el no repudio de cualquier tipo de documento electrónico. [KAUR, 2012]

- El sellado de tiempo es el único mecanismo que puede dar fe y confianza en la fecha y hora en los que unos datos han existido y no han sufrido modificación alguna. [STAPLETON, 2005]
- La verificación de la firma digital es una operación compleja que desencripta el hash encriptado y hace la comparación con el hash obtenido al momento de la verificación, si ambos has son iguales entonces el documento no ha sufrido ninguna modificación y se confía en su integridad y autenticidad [KULKARNI, 2014].
- El middleware es un componente software que permite la interpretación de las instrucciones de un dispositivo criptográfico con una aplicación de alto nivel como la firma digital. [FU, 2011]
- Para la aplicación de este modelo, se consideró los aspectos técnicos mínimos soportados tanto en el lado cliente como en el lado servidor [BIT4ID, 2015].
- La tecnología PKI brinda total seguridad y garantía de que cualquier tipo de información que se encuentre firmada digitalmente sea íntegra y autentica.
- Todo nuevo cambio tecnológico o paradigma involucra un esfuerzo perpetuo para que los usuarios utilicen la tecnología de manera adecuada. Si bien el uso de la firma y los certificados digitales se encuentra respaldado por el Estado Peruano, aún no se hace un uso extensivo u obligatorio, pues es un proceso paulatino y constante hasta que todas las entidades públicas y privadas puedan ofrecer servicios digitales a través de la tecnología PKI.
- La tecnología cumple en este caso el rol de facilitar y optimizar los procesos, pero depende en gran medida del uso adecuado del usuario final.
- La firma digital puede ser modificada a través de algunas herramientas, pero siempre dejará evidencia de cualquier modificación al momento de ser validada, y no se podrá confiar del contenido de la firma.
- Se sugiere una autenticación fuerte (o de doble factor), basada en certificados digitales, para el acceso a la intranet de la Municipalidad de Miraflores.
- Se recomienda el uso de certificados digitales SSL a nivel de servidor esto permite garantizar un canal seguro y cifrado entre el servidor y navegador web.
- Este trabajo podrá ser replicado en cualquier otra institución que disponga de un flujo de trabajo basado en web.

7.2. TRABAJOS FUTUROS

- El siguiente trabajo será implementar el algoritmo SHA 2 para la generación de firma digital a partir del 1ro de Enero del 2017 según Resolución Nº 042-2016/CFE-INDECOPI.
- La posibilidad de acceder a certificados digitales remotos contenidos en un dispositivo criptográfico HSM, permitiendo al usuario la total libertad de portar un token criptográfico y smart card (tarjetas inteligentes).
- Poder realizar la implementación de este modelo en las diferentes entidades públicas y privadas del estado peruano.

REFERENCIAS BIBLIOGRÁFICAS

[BIT4ID, 2015] Best Information Technology for Identification. (Disponible en: http://www.bit4id.com/es/). Consultado el 16/11/2015.

[BUCCAFURRI, 2008] Signing the Document Content is not enough: A new Attack to Digital Signature. 978-1-4244-2624-9/08/$25.00 ©2008 IEEE. Pg. 52- 525.

[CÁNOVAS, 2002] Cánovas Reverte, Óscar (2002). Propuesta de una Infraestructura de Clave Pública y su Extensión Mediante un Sistema de Gestión Distribuida de Credenciales Basado en Delegación y Roles (Tesis para la obtención del grado de Doctor). Murcia: Universidad de Murcia – Facultad de Informática.

[CIPHER, 2012] CRYPTOGRAPHIC OPERATION, Public Key Infrastructure (PKI) (Disponible en: http://www.cipher.risk.tsukuba.ac.jp/?page_id=609&lang=en). Consultado el 09/09/2015.

[CODESI, 2011] COMISIÓN MULTISECTORIAL PARA EL DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN (2011). Plan de Desarrollo de la Sociedad de la Información del Perú: Agenda Digital 2.0. (Disponible en: http://www.codesi.gob.pe/docs/AgendaDigital20_28octubre_2011.pdf) Consultado el: 08/10/2015.

[CONGRESO DE LA REPÚBLICA DEL PERÚ, 2001] Ley N° 27269, Ley de Firmas y Certificados digitales.

[CYBERSEC, 2013] Cybersec Consult S.A. (Disponible en: http://www.cybersec.com.pe/produc.html). Consultado el: 16/11/2015.

[DAMGARD, 1990] Damgård, I (1990). A design principle for hash functions. *Advances in Cryptology - Crypto '89*, Springer-Verlag (1990), 416-427.

[EL PERUANO, 2011] Decreto Supremo que modifica el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo N°681 y ampliatorias. Pág. 447328 – 447329.

[EL PERUANO, 2012] Establecen disposiciones para facilitar la puesta en marcha de la firma digital y modifican el Decreto Supremo Nº 052-

2008-PCM Reglamento de la Ley de Firmas y Certificados Digitales. Pág. 476913 – 476914.

[ETSI, 2009] ETSI TS 102 778-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES.

[ETSI, 2010] ETSI TS 101 903 V1.4.2 - Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES).

[ETSI, 2012] ETSI TS 101 733 V2.1.1 - Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES).

[FIRMAPROFESIONAL, 2016] Disponible en https://www.firmaprofesional.com/esp/. Consultado el 20/04/2016

[FU, 2011] Research and implementation of a digital signature schema based on middleware. Computer and Software Institute. Nanjing University of Information Science and Technology, Nanjing, China. IEEE pg.2468 -2471.

[GAIKWAD, 2015] Gaikwad, A. P. (2015). Role of Digital Signature for Authentication of E-Documents. *International Journal of Scientific Research*, Volumen: 4, Issue: 1. January 2015 ISSN No 2277 – 8179, p. 68-70.

[GARCIA, 2008] García Rojas, W. A. Implementación de Firma Digital en una Plataforma de Comercio Electrónico . Lima: Pontificia Universidad Católica del Perú - Facultad de Ciencias e Ingeniería.

[HUN, 2012] Hun Myoung Park. The web Accessibility Crisis of the Korea's Electronic Government: Fatal Consequences of the Digital Signatures Law and Public Key Certificate. International University of Japan. 978-0-7695-4525-7/12 $26.00 2012 IEEE.

[IETF, 2013] X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol. Disponible en: https://www.rfc-editor.org/rfc/pdfrfc/rfc6960.txt.pdf. Consultado el: 16/10/2015.

[INDECOPI, 2007] IOFE, "Guía de Acreditación de Entidades de Certificación EC" Versión 3.3, Rev: 03/23-02-2007.

[INDECOPI, 2007A] IOFE, "Guía de Acreditación de Entidades de Registro ER" Versión 3.3, Rev: 03/23-02-2007.

[INDECOPI, 2008] IOFE, “Guía de Acreditación de Aplicaciones de Software” Versión 3.4, Rev: 05/04-02-2008.

[INDECOPI, 2015] (Disponible en: http://www.INDECOPI.gob.pe/0/modulos/JER/JER_Interna.aspx?are=0&pfl=6&jer=1310 . Consultado el: 07/07/2015).

[INTYPEDIA, 2010] Information Security Encyclopedia. Un proyecto de la Universidad Politécnica de Madrid UPM. (Disponible en: http://www.intypedia.com/. Consultado el: 09/10/2015).

[KAUR, 2012] Digital Signature. Guru Nakar Dev University, India. 978-0-7695-4817-3/12 $26.00 © 2012 IEEE

[KULKARNI, 2014] Kulkarni, S., Chole, V. y Prasad, P. S (2014). Review on Authentication Mechanisms of Digital Signatures used for Certification. *IJCSMC*, Vol. 3, Issue. 2, February, p.735 – 738.

[KUPPUSWAMY, 2012] Kuppuswamy, P., Mohammad Appa, P. y Al-Khalidi, S. Q. Y. (2012). A New Efficient Digital Signature Scheme Algorithm based on Block cipher. *IOSR Journal of Computer Engineering*, ISSN: 2278-0661, ISBN: 2278-8727 Volume 7, Issue 1 , Dec. 2012, p. 47-52.

[MARKANTONAKIS, 2009] Markantonakis, K., Tunstall, M., Hancke, G., Askoxylakis, I. y Mayes, K. (2009). Attacking smart card system: Theory and practice. Information Security Technical Report.

[MUNICIPALIDAD DE MIRAFLORES, 2015] Portal de Transparencia. (Disponible en: http://www.miraflores.gob.pe/_transparencia.asp?mm=miraflores. Consultado el 16/11/2015).

[NA, 2008] Na Zhu, GouXi Xiao.The Application of a Schema of Digital Signature in Electronic Government. Hebei University of Technology, Tianjin, China. IEEE pag. 618-621

[NAUMANN, 2009] Ingo Naumann, Giles Hogben, “Privacy Features of European eID Card Specifications”, Version: 1.0.1 | Date: 2009-01-27.

[NCRYPTOKI, 2014] Ncryptoki, Ugo Chirico. (2014). (Disponible en: http://www.ncryptoki.com/. Consultado el: 14/08/2014).

[NIST, 1998] Public Key Infrastructure (PKI) Technical Specifications: Past A – Technical Concept of Operations. (Disponible en: http://csrc.nist.gov/archive/pki-twg/baseline/pkicon20b.PDF. Consultado el: 10/10/2015).

[NIST, 2011] Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST Special Publication 800-131A, January 2011.

[NIST, 2014] National Cyber Awareness System: Vulnerability Summary for CVE-2013-2465. (Disponible en: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2465. Consultado el 09/10/2015).

[NIST, 2015] Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules. (Disponible en: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm. Consultado el: 08/07/2015).

[NOROOZI, 2013] Noroozi, E., Salwani, M. D. y Sabouhi, A. (2013). Secure Digital Signature Schemes Based on Hash Functions. *IJITEE* ISSN: 2278-3075, Volume-2, Issue-4, March, p. 321 - 324.

[ONGEI, 2002] Infraestructura de Llave Pública para el Estado Peruano (PKI) Framework (Disponible en: http://www.ongei.gob.pe/publica/proyectos/4821.pdf) Consultado el: 25/10/2015.

[ONGEI, 2013] Política Nacional de Gobierno Electrónico 2013-2017. (Disponible en: http://www.ongei.gob.pe/docs/Pol%C3%ADtica_Nacional_de_Gobierno_Electronico_2013_2017.pdf) Consultado el: 08/10/2015.

[PARAG, 2014] Parag, S. D. y Pande, P. (2014). A Study of Electronic Document Security. *IJCSMC*, Vol. 3, Issue. 1, January, p.111 – 117.

[PCM, 2013] Política Nacional de Modernización de la Gestión Pública al 2021.Disponible en: http: //www.pcm.gob.pe/wp-content/uploads/2013/05/PNMGP.pdf. Consultado el: 08/10/2015).

[RENIEC, 2015] (Disponible en: http://portales.RENIEC.gob.pe/web/dni/inicio. Consultado el: 07/07/2015)

[RSA, 2015] (Disponible en: http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm. Consultado el: 09/10/2015).

[RUNDGREN, 2015] Rundgren, A. (2015). Web2Native Bridge. *WebPKI.org*, V0.99, 2015-04-28.

[SANS, 2015] (Disponible en: http://www.sans.org/reading-room/whitepapers/infosec/digital-signature-multiple-signature-cases-purposes-1154. Consultado el: 07/07/2015).

[SCRIBD, 2014] (Disponible en: http://es.scribd.com/doc/106604365/DESMATERIALIZACION#scribd. Consultado el: 08/07/2015).

[SMARTCARD.CO.UK, 2015] (Disponible en: http://www.smartcard.co.uk/tutorials/sct-itsc.pdf). Consultado el: 07/07/2015.

[STAPLETON, 2005] The Digital Signature Paradox. Workshop on Information Assurance and Security. United States Minitary Academy. NY. 0-7803-9290-6/05/$20 IEEE. Pg. 456-457.

[SUBRAMANYA, 2006] Subramanya, S. R. y Byung, K. Y. (2006). Digital Signatures. 0278-6648/06/$20.00 © 2006 IEEE.

[SUNARP, 2014] SUNARP, Resolución N°234-2014-SUNARP-SN, Septiembre 2014.

[US-CERT, 2013] Alert (TA12-240A) Oracle Java 7 Security Manager Bypass Vulnerability (Disponible en: https://www.us-cert.gov/ncas/alerts/TA12-240A. Consultado el: 09/10/2015).

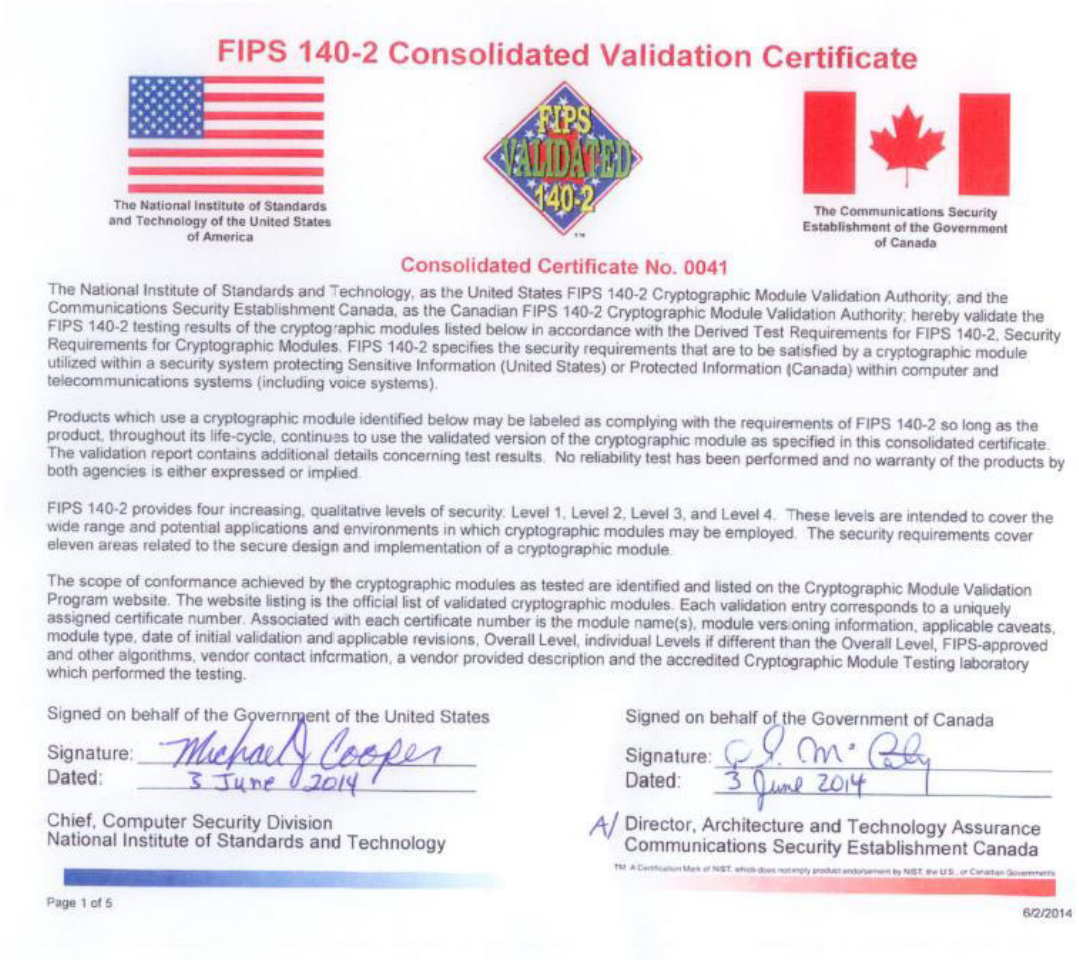
[WEBPKI.ORG, 2015] Web2NativeBridge. (Disponible en: https://cyberphone.github.io/openkeystore/resources/docs/web2native-bridge.pdf Consultado el: 07/07/2015).

[WEBTRUST, 2011] Trust Service Principles and Criteria for Certification Authorities Version 2.0 (Disponible en: http://www.webtrust.org/homepage-documents/item54279.pdf Consultado el: 07/07/2015).

ANEXOS

FIPS 140-2 Consolidated Validation Certificate

[NIST, 2015]



FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0041

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: Michael J Cooper

Dated: 3 June 2014

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: 3 June 2014

A/ Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Page 1 of 5

6/2/2014

Certificación Common Criteria EAL4+

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0422-2008

Smart Card with Digital Signature Application

Touch&Sign2048
Version 1.00

from	ST Incard S.r.l.
PP Conformance:	Protection Profile Secure Signature-Creation Device Type 3, Version 1.05, BSI-PP-0006-2002
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_MSU.3 and AVA_VLA.4

Common Criteria Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using the *Common Methodology for IT Security Evaluation, Version 2.3* extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)*

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 09. April 2008
For the Federal Office for Information Security

Bernd Kowalski
Head of Department

IT Security Certified
SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 9582-111

LEY Nº 27310

LEY QUE MODIFICA EL ARTÍCULO 11º DE LA LEY Nº 27269

EL PRESIDENTE DE LA REPÚBLICA POR CUANTO:

El Congreso de la República ha dado la Ley siguiente:

LEY QUE MODIFICA EL ARTÍCULO 11º DE LA LEY Nº 27269

Artículo Único.- Objeto de la ley

Modificase el Artículo 11º de la Ley Nº 27269, el mismo que quedará redactado de la siguiente manera:

"Artículo 11º.- Los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la presente Ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente."

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los veintiséis días del mes de junio del dos mil.

MARTHA HILDEBRANDT PÉREZ TREVIÑO
Presidenta del Congreso de la República

LUIS DELGADO APARICIO
Segundo Vicepresidente del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los quince días del mes de julio del año dos mil.

ALBERTO FUJIMORI FUJIMORI
Presidente Constitucional de la República

ALBERTO BUSTAMANTE BELAUNDE
Presidente del Consejo de Ministros y Ministro de Justicia